

Brocade Firmware Management Fundamentals

FW-120

Student Guide

Revision 0921

Copyright © 2020 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Broadcom, the pulse logo, Connecting everything, Brocade, the stylized B logo, and MyBrocade are registered trademarks of Broadcom in the United States and/or in other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

Revision: September 2021



Brocade Firmware Management Fundamentals

FW-120

0921



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Legal Disclaimer

- Broadcom, the pulse logo, Connecting everything, Brocade, and the stylized B logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Copyright © 2021 Broadcom Inc. All Rights Reserved. For product information, please visit broadcom.com.

2 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Course Introduction



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Course Overview

- This course covers the Fabric OS firmware upgrade process for Brocade Switches using the Brocade Fabric Operating System (FOS) CLI

4 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company



Course Objectives

- After completing this course, students should be able to upgrade firmware on Brocade switches and directors using the FOS CLI
 - Note: For information on using SANnav Management Portal software for updating and managing firmware on Brocade switches see the course “SANnav Management Portal Firmware Management” (course code: MPFW-220)¹

5 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: Brocade Network Advisor does not support managing SAN switches running Fabric OS v9.0.0 or later

Course Prerequisites

- Before taking this course, students should have working knowledge of Brocade Fibre Channel switches and directors

6 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.





Course Agenda

- Required Learning Elements
 - Module: Firmware Management
 - Including a firmware upgrade demonstration of a departmental switch
 - Assessment quiz
- Optional Learning Elements
 - Welcome to Brocade module
 - Student Guide (downloadable PDF)

7 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Brocade Firmware Platform Specific Downloads



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Platform Specific Downloads (PSDs)

- Historically FOS was able to run on every support HW platform, thus the FOS image could be downloaded to every platform
- Starting with Fabric OS firmware versions v8.2.2 and v9.0.1 the firmware file became platform specific, example the v9.0.1 firmware file for the G620 can not be used to upgrade firmware on a G720¹
 - This reduces the size of the file by 65-90%, which makes for a much faster download and file transfer times
 - If attempting to download a file image that is not compatible with the switch the following message will be displayed:

“Cannot download the requested firmware because the firmware doesn't support this platform. Please enter another firmware.”

9 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: SANnav Management Portal v2.1.1.3 and 2.1.1.4 patches include PSD support

Platform Specific Downloads (cont.)

- Example, the image files for Fabric OS v9.0.1b are:
- Files are available in:
 - .zip for Windows
 - or .tar.gz for Linux
- Other files include:
 - v9.0.1b.md5 → MD5 Checksum file
 - v9.0.1b.all_mibs → MIBs file
 - v9.0.1b.releasenotes → Release notes

Example Image Filename	Descriptions
v9.0.1b.EXT	7810 platform
v9.0.1b.EMB	G648 and MXG610 platforms
v9.0.1b.G6_ENTRY	G610 platform
v9.0.1b.G6_MID	G620 platform
v9.0.1b.G6_ENTP	G630 platform
v9.0.1b.G7_MID	G720 platform
v9.0.1b.G6G7_DIR	X6-8, X6-4, X7-8 and X7-4 platforms

See next notes page in
PDF for 8.2.2 firmware
image file names

10 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



See next notes slide for Fabric OS v8.x image files

8.2.2c6 platform image files:

Image Filename	Descriptions
v8.2.2c6_EXT	7840 and 7810 platforms
v8.2.2c6_G5_ENTRY	6505 platform
v8.2.2c6_G5_MID	6510 platform
v8.2.2c6_G5_ENTP	6520 platform
v8.2.2c6_G5G6_DIR	DCX 8510-8, DCX 8510-4, X6-8, and X6-4 platforms
v8.2.2c6_G6_ENTRY	G610 platform
v8.2.2c6_G6_MID	G620 platform
v8.2.2c6_G6_ENTP	G630 platform
v8.2.2c6_EMB	M6505, 6543, 6543, 6545, 6546, 6547, 6548 and 6558 platforms

- ❖ The platform image files come in zip format for windows and tar.gz format for Linux servers

Other files include:

- v8.2.2c6.md5 → Checksum file
- v8.2.2c6_all_mibs → MIBs file
- v8.2.2c6_releasenotes → Release notes

Brocade Trusted FOS (TruFOS) Certificates



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Brocade Trusted FOS (TruFOS) Certificates

- Brocade Trusted FOS (TruFOS) Certificates ensure data center environments are securely enabled to perform critical operations like firmware migration and verify the integrity and authenticity of new code before allowing changes to the Fabric OS (FOS) on SAN switches
- Guarantees that a switch is running authentic FOS code in a manner that is supported by Brocade and our OEM partners
 - Each TruFOS Certificate is tied to an individual switch, verifying that the switch and FOS image are genuine Brocade products
 - A valid TruFOS Certificate also assures the customer that the switch has current support and entitlement, so there is no concern if technical support assistance is needed

13 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Brocade Trusted FOS (TruFOS) Certificates (cont.)

- TruFOS Certificates are recognized and supported beginning with FOS v9.0.0
 - TruFOS Certificates are XML files uniquely associated with the switch License ID (LID)
 - No behaviors are affected or limited in any way by the TruFOS Certificate in FOS v9.0.x
 - The TruFOS Certificates applies to enterprise switches: G630 and all X6 and X7 directors
- A new switch shipped from the factory will a TruFOS Certificate valid for 38 months
 - A MAPS event is generated weekly starting 60 days prior to the certificate expiration date and if not renewed, monthly following the expiration date
 - Getting a TruFOS Certificate is free to all customers with current entitlement¹
 - See appendix for more information on getting and installing a TruFOS Certificate
- A TruFOS Certificate installed in the field is good for 12 months or the duration of the current support contact, whichever is less (see notes for FRU replacement)
 - A new certificate can be created at any time (see appendix for more information)

14 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: Meaning the switch has a valid support contract through either Brocade or an OEM.

Note: If a switch has to be replaced, the replacement switch will come with a 30 day TruFOS certificate as part of the existing license transfer process. User can obtain a replacement TruFOS certificate good for up to one year. See appendix for more information.

Brocade Trusted FOS (TruFOS) (cont.)

- Brocade X6 and G630 platforms upgraded from any FOS v8.x release to FOS v9.0.0 or v9.0.0a must first get and install a TruFOS Certificate prior to migrating to FOS v9.0.1x
 - See appendix for information on getting and installing a TruFOS certificate
- Brocade X7 directors have pre-installed TruFOS Certificate
- Although TruFOS Certificates do not currently enable any features or functionality, certificate status is displayed in the `license --show` command output¹
 - New or updated TruFOS Certificates can be obtained by contacting your support provider
 - If Brocade is your support provider, see the appendix for information on getting a TruFOS Certificate

15 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: Example `license --show` command output with TruFOS Certificate loaded

```
SW1:FID128:admin> license --show
License Id : 10:00:c4:f5:7c:2e:c6:91
<truncated output>
License 2 :
-----
  License serial number   : FOS-86-0-04-11203823
  License features        : Trusted FOS (TruFOS) Certificate
  Generation date         : 04/08/2021
  Expiry date             : 04/08/2022
-----
```

Migration Paths



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Fabric OS v8.2.2c Firmware Migration

- **Migrating from FOS v8.1.x**

- Any Brocade platform (except the G610) running FOS v8.1.0a or later can be non-disruptively upgraded to FOS v8.2.2c
 - On Brocade G610 the upgrade from FOS v8.1.0 to FOS v8.2.2c will be disruptive

- **Migrating from FOS v8.0.x**

- Any supported Brocade platform and X6-8/X6-4 blades¹ running any FOS v8.0 firmware must be upgraded to FOS v8.1.x firmware before it can be non-disruptively upgraded to FOS v8.2.2c
- Always check release notes for updated information

17 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: X6-8/X6-4 blade support table:

Blades	FOS v8.2.2c Support
FC32-48 32G FC blade	Supported
SX6 Gen 6 Extension blade	Supported, Up to a maximum of four blades of this type
FC32-64 32G FC/FCoE blade	Supported. A maximum of two blades of this type is supported when four SX6 blades are present in the same X6-8 chassis

Fabric OS v9.0.1x (v9.0.1a or v9.0.1b) Firmware Migration

• Migrating from FOS v9.0.0

- For Brocade X7 directors and G720 switch, upgrades from FOS v9.0.0 to FOS v9.0.1x are disruptive
 - A disruptive upgrade from FOS v9.0.0 to v9.0.1x using the `firmwaredownload` command with the `-s` option is supported
- For other platforms it is a non-disruptive upgrade from FOS v9.0.0 to FOS v9.0.1x
- **Note:** For the Brocade X6 directors and G630 switch upgraded from any of the FOS v8.x releases to FOS v9.0.0 or v9.0.0a must install a TruFOS certificate¹ prior to upgrading to FOS v9.0.1x (See appendix for information on getting and installing a TruFOS certificate)

• Migrating from FOS v8.2

- Any Brocade supported platform² running any FOS v8.2 version can be non-disruptively upgraded to FOS v9.0.1x

18 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: More information about the TruFOS certificate later in this presentation. Information about getting a TruFOS certificate can be found in the appendix.

Footnote 2: Platforms supported by Fabric OS v9.0.x

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module
- Brocade 7810 Extension Switch

See next notes page for X6 and X7 Fabric OS v9.0 supported blades

X6-8 and X6-4 Blade Support:

Blades	FOS v9.0.x Support
FC32-48 32G FC blade	Supported
SX6 Gen 6 Extension blade	Supported, up to a maximum of four blades of this type
FC32-64 32G FC/FCoE blade	Supported

X7-8 and X7-4 Blade Support:

Blades	FOS v9.0.x Support
FC32-X7-48 32G X7 FC blade	Supported
FC64-48 64G FC blade	Supported
FC32-48 32G FC blade	Supported
SX6 Gen 6 Extension blade	Supported, Up to a maximum of four blades of this type
FC32-64 32G FC/FCoE blade	Supported

Fabric OS v9.0.1x (v9.0.1a or v9.0.1b) Firmware Migration (cont.)

- **Migrating from FOS v8.1**

- Any FOS v9.0.1x supported Brocade platform¹ that is currently running any FOS v8.1.x version must be upgraded to FOS v8.2.x firmware before it can be non-disruptively upgraded to FOS v9.0.1x
- Always check release notes for updated information

20 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: The following devices are supported in this release: (Note, this list is a list of switches that are supported on FOS v9.0.1a2 (Not all of these devices are supported on FOS v8.1 (Gen 7 devices for example))

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module
- Brocade 7810 Extension Switch

Before Upgrading Brocade Switch Firmware



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Firmware Download Best Practice

- Read the release notes for the new firmware any updated information related to the firmware download process or support¹
- Refer to the Brocade Fabric OS Software Upgrade Guide, for information on:
 - Obtaining firmware
 - Upgrading and downgrading firmware considerations
 - Firmware compatibility matrix information
- Run the `firmwareshow` command to verify the current version of Fabric OS
- Run the `configupload` command to backup the current switch configuration

22 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: If this switch was purchased from an OEM vendor there may be upgrade requirements different from those listed here. Contact your vendor for additional information.

Firmware Download Best Practice (cont.)

- Run the `supportsave` command to retrieve all current core files prior to executing the firmware download
 - This helps to troubleshoot the firmware download process if a problem occurs
- Optional: For additional support, connect the switch to a computer with a serial console cable¹
 - This captures all the console message during the upgrade process
- For each switch in your fabric, complete all firmware download changes on the current switch before issuing the `firmwaredownload` command on the next switch
 - This process ensures that traffic between switches in your fabric is not disrupted
- Do not perform any configuration changes on the fabric while firmware download is in progress

23 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: Ensure that all serial consoles (both CPs for directors) and any open network connection sessions, such as Telnet, are logged and included with any trouble reports.

Downloading Firmware



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Downloading Firmware

- Access to Brocade Fabric OS firmware is available for customers with support service contracts and for partners on the website at: <https://www.broadcom.com>
- Perform the following procedure to download the firmware and documentation files from the website:
 1. From the website <https://www.broadcom.com>, click **LOGIN**, and enter your username and password
 - If you do not have an account, click REGISTER to set up your account
 2. Under MyApps, click on **docSAFE**
 3. Click on the **Product Search box** to open the pull down menu and click on **Brocade Storage Networking**
 - The list of firmware and documents available for the product appears
 - Click the **Download ICON** (far right side of the page) to download the firmware or documentation
 4. Uncompress the firmware file

25 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



End User License Agreement (EULA) Acceptance



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

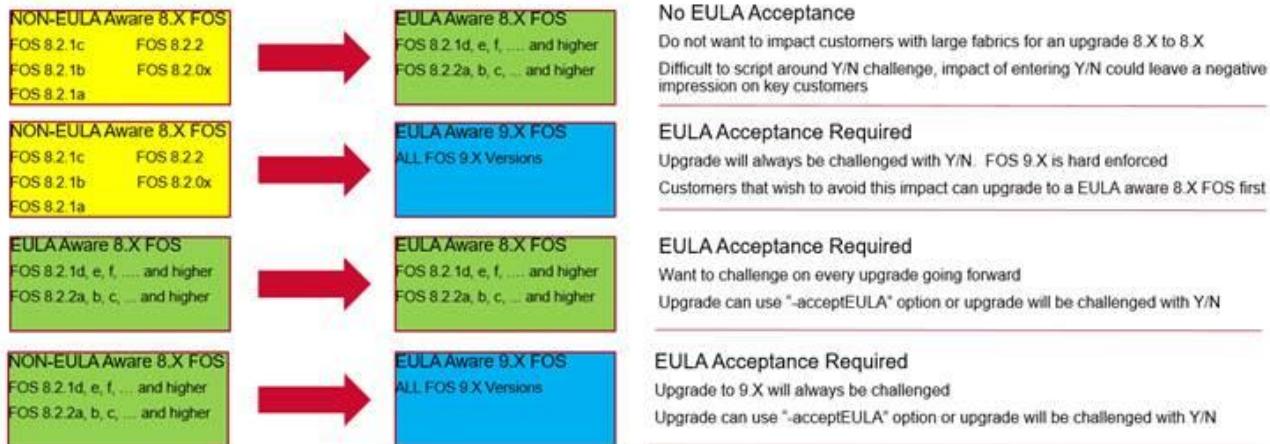
End User License Agreement (EULA)

- On any Brocade SAN switch, firmware upgrade to Fabric OS v9.0.0 or later must accept the EULA before the Fabric OS can be installed
- On any Brocade SAN switch running Fabric OS v9.0.0 or later, firmware upgrade or downgrade must accept the EULA before Fabric OS can be installed
 - Example going from Fabric OS v9.0.0 to v9.0.1b the EULA must still be accepted
- See notes for additional information on pre-Fabric OS v9.0 EULA requirements
- A PDF copy of the End User License Agreement can be downloaded from docSAFE, the name of the document is: "Brocade Fabric Operation System and Feature Licenses and License keys"

27 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



FOS 8.x EULA Acceptance



Display the End User License Agreement (EULA)

- For switches running Fabric OS v9.0.0 or higher to display the EULA run command `firmwaredownload -showEULA` command
 - Note: The `-showEULA` option is case sensitive

```
X7-4:FID128:admin> firmwaredownload -showEULA
*****
* BROCADE FABRIC OPERATING SYSTEM AND FEATURE LICENSES AND LICENSE KEYS *
*****
END USER LICENSE AGREEMENT
=====
THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE DOWNLOAD, INSTALLATION,
USE, POSTING, DISTRIBUTING AND OTHERWISE MAKING AVAILABLE OF BROCADE'S FABRIC
OPERATING SYSTEM ("FOS") SOFTWARE AND/ OR USE OF BROCADE FEATURE LICENSES AND
LICENSE KEYS THAT ACTIVATE FOS OR FUNCTIONALITY WITHIN FOS, AND ACCOMPANYING
DOCUMENTATION (collectively the "Software").
```

<truncated output>

28 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Acceptance of the End User License Agreement (EULA)

- In this example the user is upgrading a G620 switch from Fabric OS v8.2.1 to v9.0.1b, notice the user must accept the EULA stipulations

```
G620:admin> firmware download
Server Name or IP Address: 10.124.91.56
User Name: FW_Admin
File Name: /v9.0.1b.G6_MID
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 2
Password:
Please acknowledge that you have read and accept Broadcom's EULA stipulations.
Please respond (Y/y=accept, N/n=do not accept, or (S/s) to show the EULA)
```

- Enter y to accept
- Enter n to not accept (which will result in the firmware not being upgraded)
- Enter s to display the EULA (After the EULA is displayed the user again will be given the chance to accept or no accept the agreement)

29 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

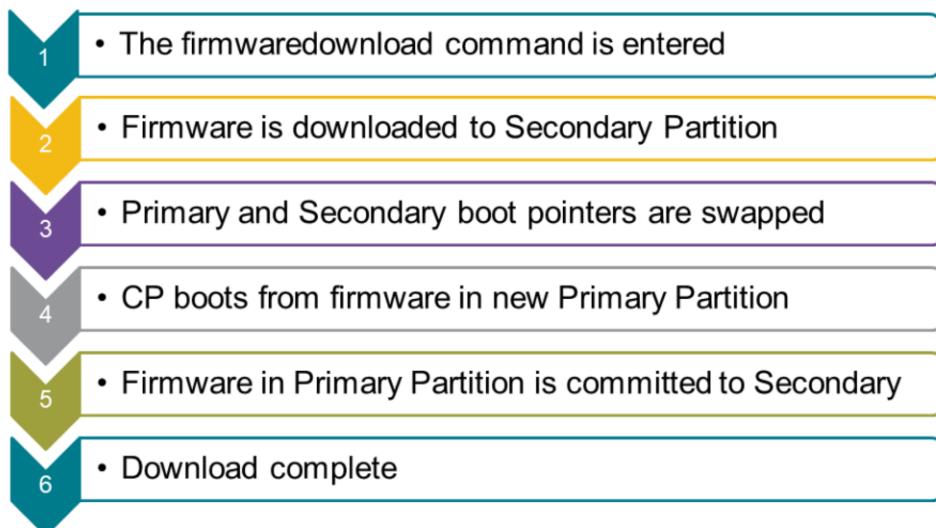


Firmware Download on Departmental Switches



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Firmware Download Internal Process

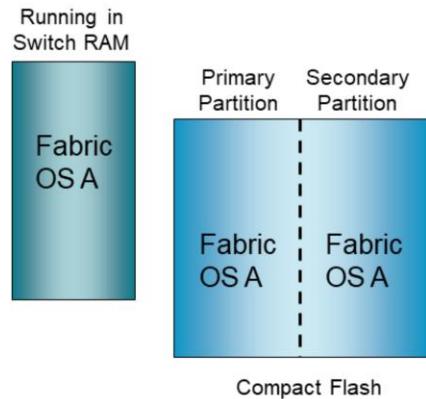


31 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



The firmware download process is the same for all of Brocade's SAN switches. Firmware is stored in flash on two separate partitions, primary and secondary. Firmware is first downloaded to the secondary partition and the switch rebooted from the updated code. This allows an opportunity to assess the new firmware and ensure that there are no problems. Once the switch has booted successfully from the update code it is then copied to the remaining flash partition.

Check Current Firmware Status



- Run the `firmwareshow` command to see the current firmware levels of each partitions:
 - Make sure both partitions are running the same version¹

```
G720:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS       v9.0.0
v9.0.0
```

32 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



The firmware download process for a single-CP (departmental) switch is less complex than the Brocade directors.

The flash is divided into two equal size partitions. The version of firmware running on the switch is in the Primary Partition. The version in the Secondary can be the same as the Primary or different.

The following slides will illustrate the individual steps that occur when a `firmwaredownload` command is issued.

Footnote 1: If not run either the one of the below commands to set both partitions to the same level of firmware:

- `firmwarecommit` – Copy firmware from the primary partition to the secondary partition (no reboot)
- `firmwarerestore` – Copy firmware from the secondary partition to the primary partition (switch reboots)



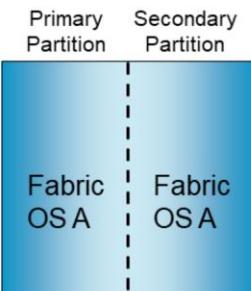
The **firmwaredownload** Command

```
G720:admin> firmwaredownload  
10.124.91.56,admin,/v9.x/v9.0.1b.G7_MID,password
```

- Where the address is the IP address of the server

Running in
Switch RAM

Fabric
OS A



Compact Flash



BROCADE
A Broadcom Company

33 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

The **firmwaredownload** command is issued to download Fabric OS version v8.0.1.

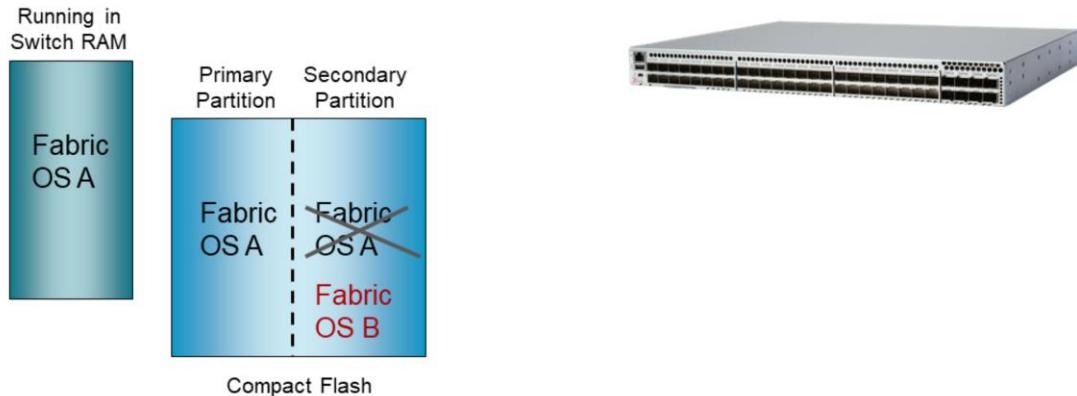
The default **firmwaredownload** settings are to auto-reboot and auto-commit. If the **-s** option is used and auto-boot mode is not enabled, a reboot command must be issued to activate the downloaded firmware. If the **-s** option is used and auto-commit mode is not enabled, a **firmwarecommit** command must be issued to replicate the downloaded firmware to the Secondary Partition.

Current status: Firmware Fabric OS A is in the Primary Partition and has been committed to the Secondary Partition.

2

Firmware Downloaded to Secondary Partition

- Firmware is downloaded to Secondary Partition

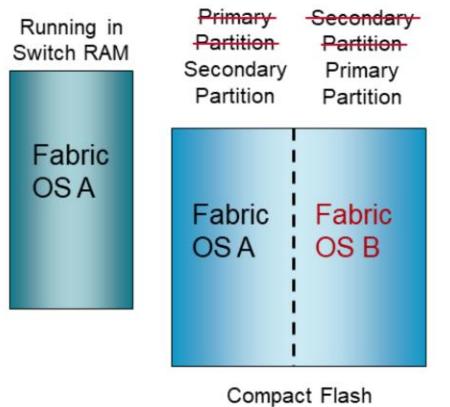


34 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Primary and Secondary Pointers are Swapped

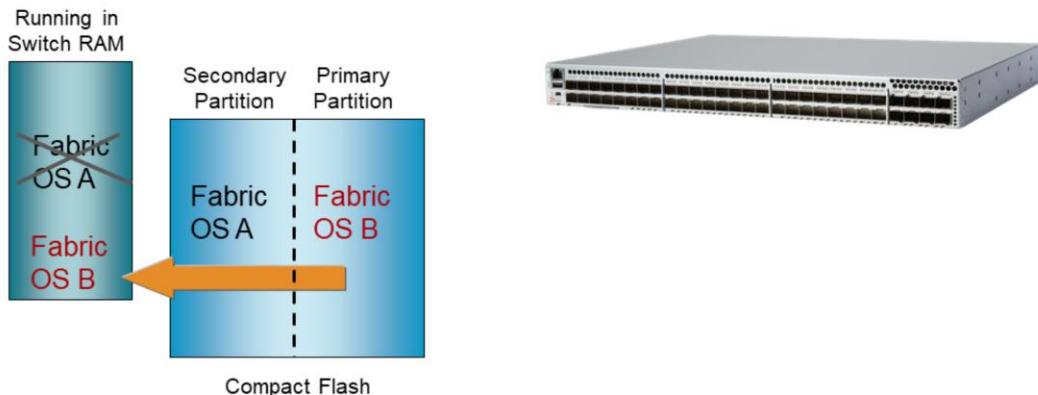
- Once the firmware has been downloaded to the Secondary Partition, the partition pointers are swapped (Secondary Partition becomes the Primary Partition and visa versa):



So now the Primary Partition contains the updated firmware, but the switch (RAM) is still running the old version at the point in the process

New Firmware Reboots

- Switch reboots¹ (non-disruptive to SAN traffic) and loads the updated firmware from the Primary Partition so now the switch is running the updated Fabric OS version



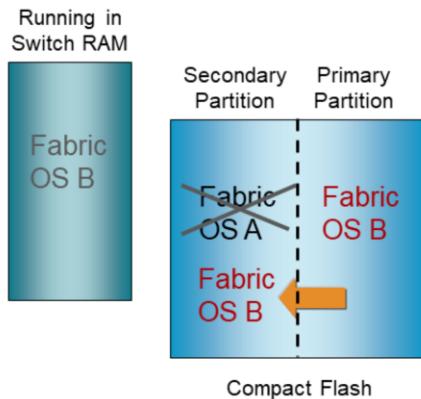
36 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Footnote 1: The reboot performed in this case is an hareboot which is non-disruptive to SAN traffic.

New Firmware Commits

- New Fabric OS version is committed from the Primary Partition to the Secondary Partition



37 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Firmware Download is Complete

Success!

Running in
Switch RAM

Fabric
OS B

Secondary
Partition Primary
Partition

Fabric
OS B Fabric
OS B

Compact Flash



Notice that the switch (RAM) and
both partitions are now running
the updated version of Fabric OS

G720:admin> **firmwareshow**
Appl Primary/Secondary Versions

FOS

v9.0.1b
v9.0.1b

BROCADE
A Broadcom Company

38 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Fabric OS v9.0.x Departmental Switch Firmware Upgrade Example

- Example upgrade of a G720 switch from Fabric OS v9.0.0 to Fabric OS v9.0.1b

```
G720:admin> firmwaredownload  
Server Name or IP Address: 10.124.91.56  
User Name: FW_Admin  
File Name: /v9.0.1b.G7_MID
```

Note: Fabric OS v9.0.x supports:
FTP, SCP, SFTP and HTTP protocols¹

```
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 2
```

```
Password:
```

```
Please acknowledge that you have read and accept Broadcom's EULA stipulations.
```

```
Please respond (Y/y=accept, N/n/do not accept, or (S/s)2 to show the EULA) Y
```

```
Checking system settings for firmwaredownload...
```

```
System settings check passed.
```

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

```
This command will cause a warm/non-disruptive boot but will require that existing telnet,  
secure telnet or SSH sessions be restarted.
```

```
Do you want to continue (Y/N) [Y]: Y
```

```
Firmware download in progress, please wait.
```



39 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Footnote 1: HTTP support was added in Fabric OS v9.0.0

Footnote 2: For some versions of firmware this will show up as a D/d options for “display” the End User License Agreement.

Note: See next notes slide for firmwaredownload command usage information

The firmwaredownload command usage:

```
X7-4--:FID128:admin> firmwaredownload -h
firmwaredownload: unrecognized option '-h'
firmwaredownload Usage: [options] [<host>, <user>, path<, password>]
Options:
  -acceptEULA      Confirms acceptance of EULA.
                    User will be prompted to accept EULA if this option
                    is not specified.

  -showEULA        Display of EULA agreement.

  -U               Download firmware from USB device on active CP (if
                  supported)

  -s               Single mode enable

  -b               Auto-reboot after firmware download completes. Use with
                  "-s" option

  -n               Disable auto-commit. Use with "-s" option

  -p               Protocol to use for firmware download. Valid options are
                  <ftp|scp|sftp|http>

  -A               Authentication Method for protocol. Valid options are
                  <cra>. Use with SCP protocol

  -o               Bypass the checking of Coordinated HotCode Load.

  -m               Server Port number. Valid only if the protocol is scp or
                  sftp or http.

  -k               Enable SFTP StrictHostKeyChecking. Valid only if the
                  protocol is scp or sftp.

  -r               Download firmware on secondary partition without
                  activation

  -l               Download firmware on local CP. Use with "-r" option

  -L               Legacy firmware download.5
```

Run the command without arguments for interactive mode.

Checking the Firmware Download Status

- Run the `firmwareDownloadStatus` command to see the status of the firmware download:

```
G720:admin> firmwareDownloadStatus
[1]: Tue Aug  5 10:29:01 2021
Firmware is being downloaded to the switch. This step may take up to 30
minutes.

[2]: Tue Aug  5 10:38:46 2021
The internal firmware image is relocated successfully.

[3]: Tue Aug  5 10:38:46 2021
Firmware has been downloaded to the secondary partition of the switch.

[4]: Tue Aug  5 10:40:04 2021
The firmware commit operation has started. This may take up to 10
minutes.
```

41 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Checking the Firmware Download Status (cont.)

- Continuing to look at the `firmwaredownloadstatus` command output:

```
[5]: Tue Aug 5 10:43:32 2021
```

```
The commit operation has completed successfully.
```

```
[6]: Tue Aug 5 10:43:32 2021
```

```
Firmwaredownload command has completed successfully. Use firmwareshow to verify the firmware versions.
```

- Display the Fabric OS versions for each partition by running the `firmwareshow` command:

```
G720:admin> firmwareshow
```

```
Appl Primary/Secondary Versions
```

```
-----
```

```
FOS v9.0.1b
```

```
v9.0.1b
```



The screenshot shows a terminal window titled "10.124.91.24 - PuTTY". The window displays a Fabric OS login session:

```
Fabric OS (demo_switch)
Fabos Version 8.2.1b

Place-MOTD-Here

• In
demo switch login: admin
Password:
This is just a test
demo_switch:FID128:admin>
```

To the left of the terminal window, there is a vertical red bar containing the text "Fire" at the top and "ee" at the bottom. At the bottom of the slide, there is a small footer with the text "43 | DE" and a red logo.

Firmware Download on Directors



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Non-disruptive Firmware Download Requirements

- For a non-disruptive CP card failover during the firmware download process:
 - Two CP cards must be installed with the same firmware on each
 - Both CP cards must be healthy
 - HA Monitor synchronized between the CP cards
 - Each CP must have a network connection
- Monitor High-Availability (HA) status using the `hashow` command, and look for:¹
 - Which CP is active? Which CP is standby?
 - Is the standby CP healthy? (ready to become the Active CP)
 - Is HA enabled between the CP cards?
 - Is the heartbeat up?
 - Are the HA monitors on the CPs synchronized?

X7-4:admin> `hashow`

```
Local CP (Slot 1, CP0): Active, Cold Recovered  
Remote CP (Slot 2, CP1): Standby, Healthy  
HA enabled, Heartbeat Up, HA State synchronized
```

See notes for additional information on meaning of the `hashow` command output



45 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Footnote 1: If the `hashow` command output shows any problems with the HA status of the CPs do not continue with any firmware upgrades until the issue is resolved.

The `hashow` command displays many details about the current high-availability status of the Brocade director including:

- Local CP state (slot number, CP ID): Active or Standby
- Remote CP state (slot number, CP ID): Active or Standby
- High Availability: HA Enabled or HA Disabled
- Heartbeat: Up or Down
- Health of standby CP: Healthy (standby CP is running, and the health monitor has not detected any errors), Failed (standby CP is running, but the health monitor has discovered a problem with the blade), and Unknown (the standby CP does not exist, the heartbeat is down, or the health monitor detects a configuration file error).
- HA synchronization status: HA State Synchronized (the system is currently fully synchronized; a CP Card failover would be non-disruptive) and HA State Not In Sync (the system is unable to synchronize the two CPs, due to the standby CP being faulty or another system error; a CP Card failover would be disruptive).

More information on the next notes slide:

Active CP state:

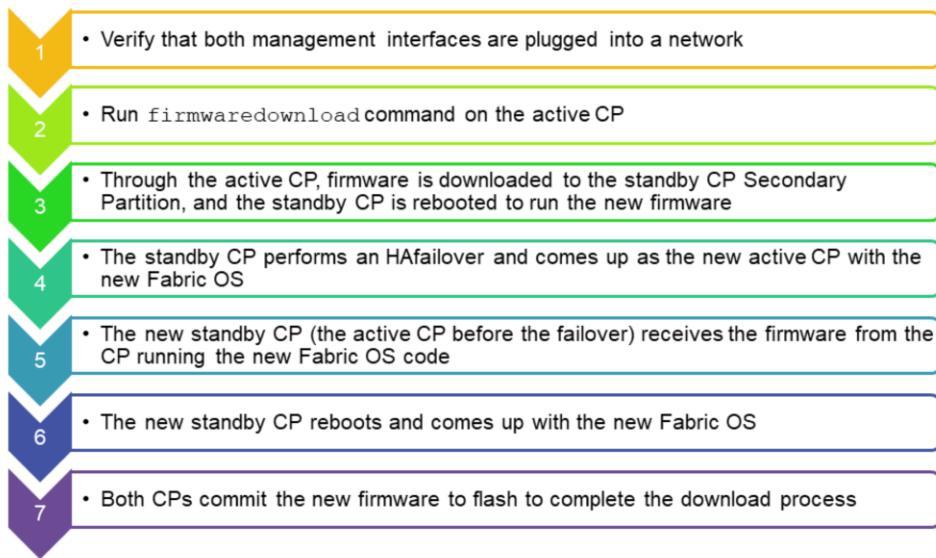
- **Cold Recovered** — The CP became the Active CP through a power on or hard reboot and is disruptive.
- **Warm Recovered** — The CP became the Active CP through a CP failover and is non-disruptive.

Standby CP state:

- **Healthy** — The Standby CP is running and the background health diagnostic has not detected any errors.
- **Failed** — The Standby CP is running but the background health diagnostic has discovered a problem with the blade. Failover is disabled until the Standby CP is repaired. Information about the failure for the Standby CP is displayed.
- **Unknown** — The Standby CP health state is unknown for one of the following reasons:
 - Standby CP does not exist, heartbeat is down
 - The Health Monitor has detected a configuration file error

See appendix for additional HA commands

Director Firmware Upgrade Overview



47 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company



Pre-Steps: hashow and firmwareshow

- Recommended best practice:
 - Run the `hashow` command and verify that HA is enabled, heartbeat is up and both CPs are in sync

```
X7-4:admin> hashow
Local CP (Slot 6, CP0): Active, Cold Recovered
Remote CP (Slot 7, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

- Use the `firmwareshow` command to verify the version of Fabric OS currently running (All partitions must be at the same version level)

```
X7-4:admin> firmwareshow
Slot Name      Appl     Primary/Secondary Versions      Status
-----          ---      ---                                ---
 1  CP0        FOS      v9.0.0
                           v9.0.0
                           v9.0.0
                           v9.0.0
 2  CP1        FOS      v9.0.0
                           v9.0.0
                           v9.0.0
                           v9.0.0
```

BROCADE
A Broadcom Company

48 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Active CP state:

Cold Recovered — The CP became the Active CP through a power on or hard reboot and is disruptive.

Warm Recovered — The CP became the Active CP through a CP failover and is non-disruptive.

Standby CP state:

Healthy — The Standby CP is running and the background health diagnostic has not detected any errors.

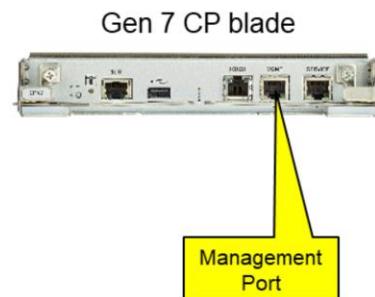
Failed — The Standby CP is running but the background health diagnostic has discovered a problem with the blade. Failover is disabled until the Standby CP is repaired. Information about the failure for the Standby CP is displayed.

Unknown — The Standby CP health state is unknown for one of the following reasons:
Standby CP does not exist, heartbeat is down
The Health Monitor has detected a configuration file error



Pre-Steps: Management Interfaces

- Verify that the management interface from each CP has a network connection
- During the firmware download process, the CPs will reboot switching between active and standby
- This management interface keeps the active and standby attached to the network
- If the management interfaces are not connected, then the firmware download will fail

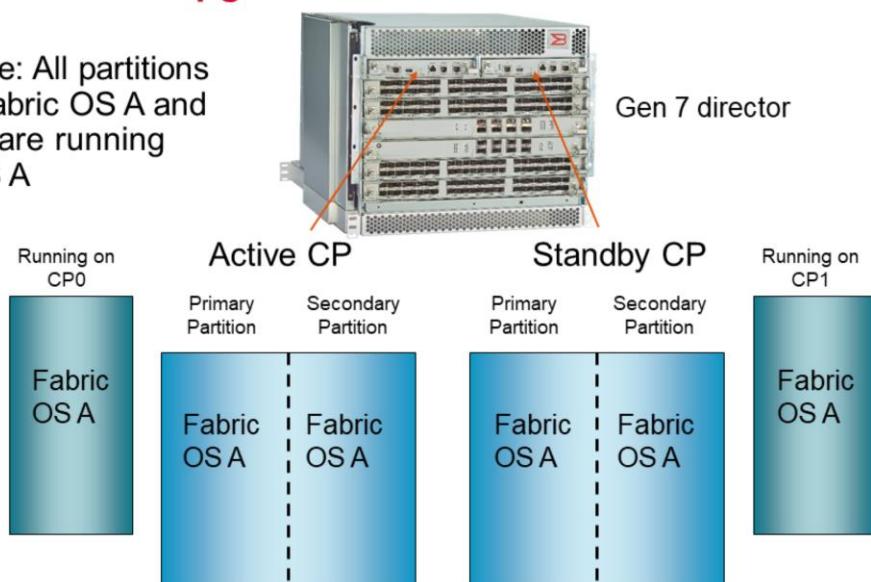


49 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Director Firmware Upgrade

- Initial State: All partitions contain Fabric OS A and both CPs are running Fabric OS A



BROCADE
A Broadcom Company

50 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

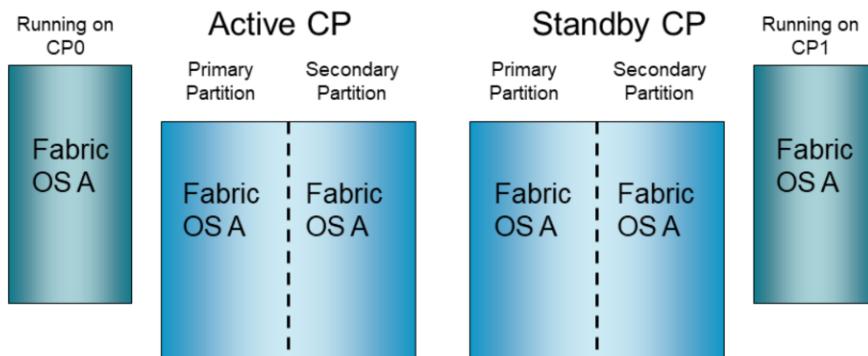
The firmware download process for a Brocade director is more complex than other Brocade switches. The director has dual Control Processor cards (CP0 and CP1) with one performing an active role and the other a standby role.

Each CP card has two compact flash cards that hold the Fabric OS firmware. The version of the firmware controlling the switch is in the primary partition and another version of firmware is kept in the secondary partition. The version in the secondary partition can be the same as the primary or different.

This is what makes the firmware process more complex. The following slides will illustrate the individual steps that occur when a `firmwaredownload` command is issued on a Brocade director.

Run `firmwaredownload` Command on the Active CP

- X7-4:admin> **firmwaredownload**
10.124.91.56,admin,/v9.x/9.0.1b.G6G7_DIR,password
– Command needs to be ran from the Active CP



51 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

The `firmwaredownload` command is issued from the Active CP to download Fabric OS version “Fabric OS B”.

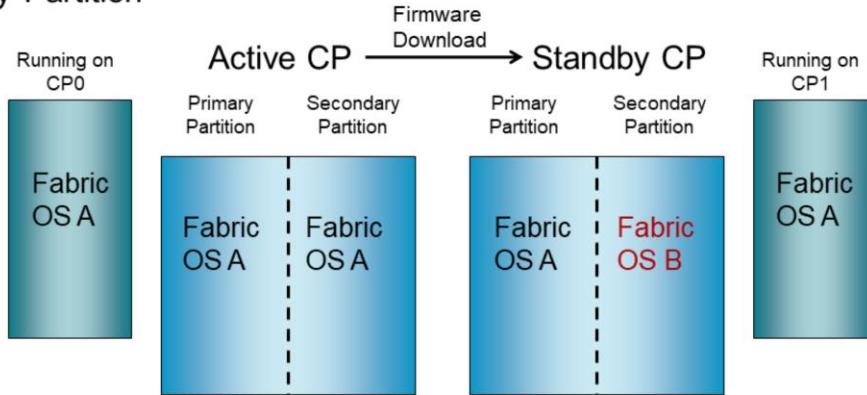
The default `firmwaredownload` options are automatically executed. The default settings are to auto-reboot and auto-commit. If the `-s` option is used and auto-boot mode is not enabled, a reboot command must be issued to activate the downloaded firmware. If the `-s` option is used and auto-commit mode is not enabled, a `firmwarecommit` command must be issued to replicate the downloaded firmware to the secondary partition.

Current status:

- The Active CP is CP0; the Standby CP is CP1
- Firmware Fabric OS A is in the primary partition and is committed to the secondary partition on both CP cards

Active CP Instructs Standby CP to Download

- Running the `firmwaredownload` command on the Active CP downloads the firmware (Fabric OS B, via the active CP management port) to the Standby CP Secondary Partition



52 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

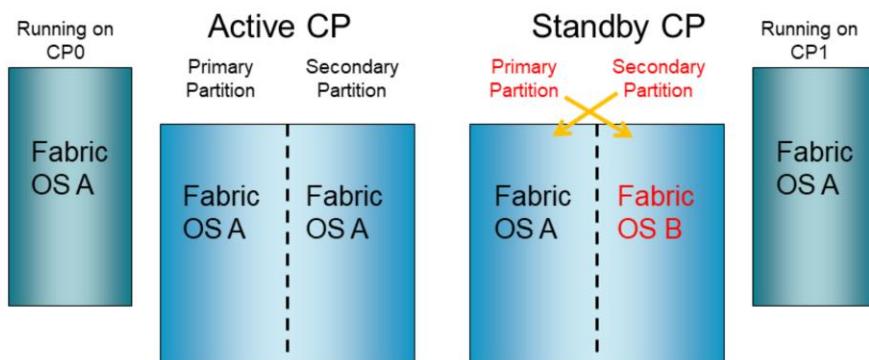
BROCADE
A Broadcom Company

The Active CP instructs the Standby CP to perform a firmware download of version Fabric OS B. The firmware is downloaded into the secondary partition. If the Standby CP does not respond within 10 minutes, the Active CP will time out and abort the command.

All Brocade directors download firmware to the Standby CP card first. Before the firmware download process begins, Fabric OS checks to see that both CP cards are running the same version of Fabric OS. If they are running different versions, each CP card will have to be updated separately.

Primary/Secondary Partitions Swapped

- On the Standby CP, the partition pointers are swapped¹, so it will be the Standby CP Primary Partition that will contain Fabric OS B²



53 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

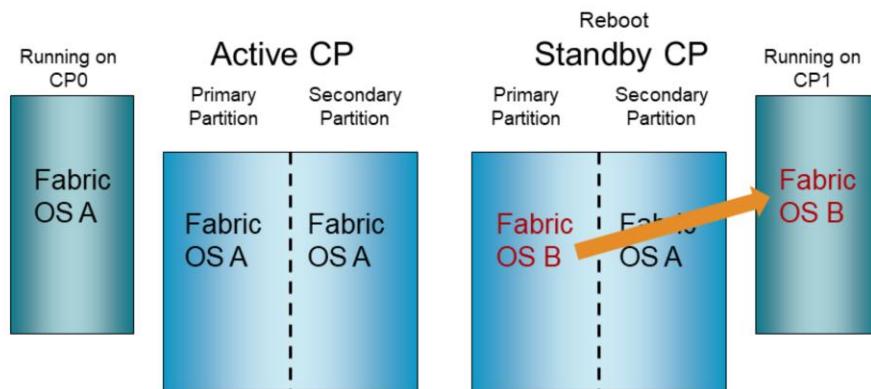
BROCADE
A Broadcom Company

Footnote 1: This is done by just updating the partition pointers.

Footnote 2: At this point the new firmware has been copied to the secondary partition on the Standby CP. The CP prepares to reboot with the new code by swapping the pointers for the primary and secondary partitions. The secondary partition becomes the primary and vice-versa.

Standby CP Performs a Reboot

- The Standby CP performs a reboot (loads the new firmware from the primary partition) which results in the Standby CP (CP1) running Fabric OS B

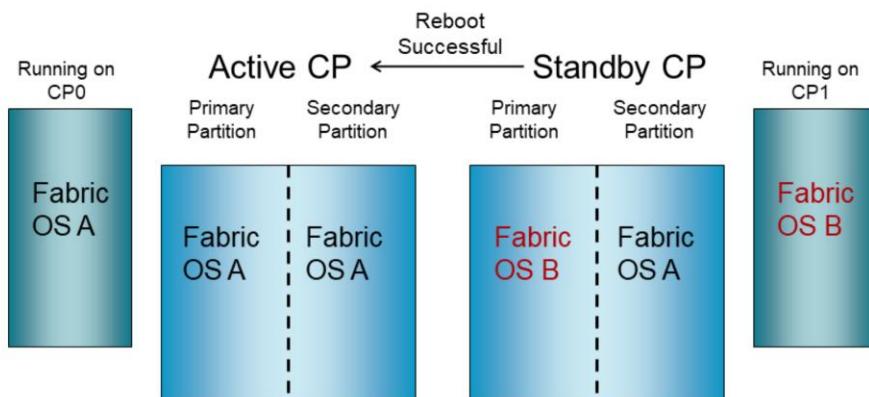


54 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

Standby CP Synchronizes with Active CP

- Once the reboot of the Standby CP (CP1) is completed, it will resync with the Active CP¹



55 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

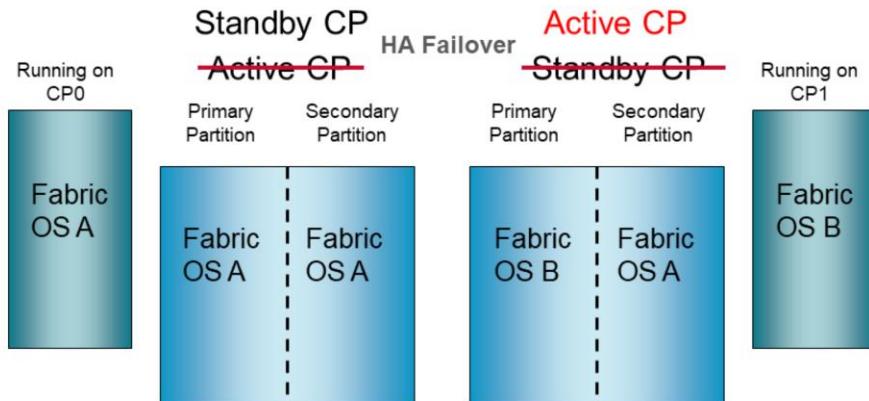
BROCADE
A Broadcom Company

Footnote 1: The standby CP is now running the upgraded Fabric OS code. It sends status back to the Active CP that the reboot was successful. The CP heartbeat is up and the CPs are communicating with each other.

Note: The CP verifies the hasync and heartbeat is up before an hafailover occurs.

HA Failover

- HA Failover occurs, which results in the CP1 (Running Fabric OS B) becoming the Active CP



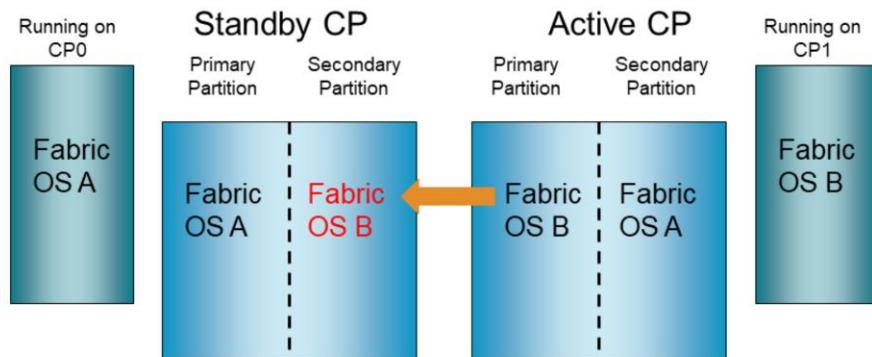
56 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

With the Standby CP now running the new firmware, a failover is performed. The Standby CP becomes Active and the Active CP becomes the Standby.

Firmware Copied from Active to Standby CP

- Next the Fabric OS B is copied from the Primary Partition on the Active CP to the Secondary Partition on the Standby CP



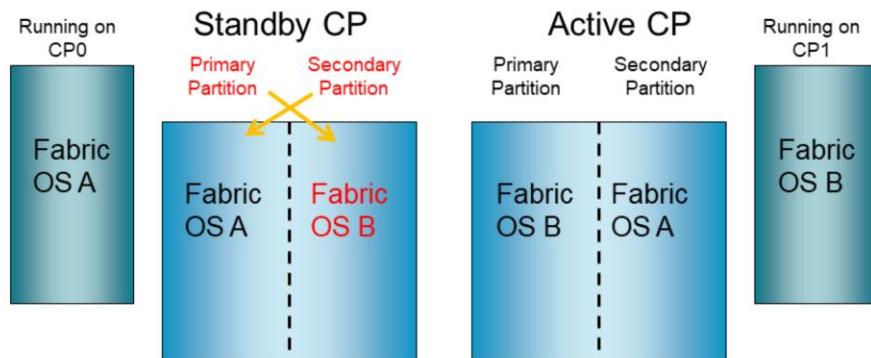
57 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

The Active CP copies the firmware from the primary partition to the secondary partition of the Standby CP using the internal network between the CP blades.

Primary/Secondary Partitions Swapped

- On the Standby CP, the partitions are swapped¹, so it will be the Standby CP Primary Partition that will contain Fabric OS B



58 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

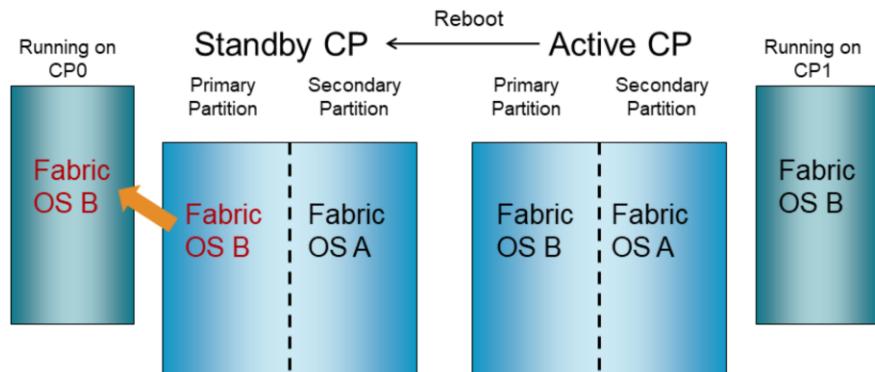
BROCADE
A Broadcom Company

Footnote 1: This is done but just updating the partition pointers.

Standby CP Reboots

- The Standby CP performs a reboot (loads the firmware from the primary partition) which results in the Standby CP (CP0) running Fabric OS B, once complete CP0 (standby) will resync with CP1 (active)

- So at this point both primary partitions contain the new firmware (Fabric OS B), and both CPs are running the new firmware (Fabric OS B)
- Notice both Secondary partitions still contain Fabric OS A



59 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

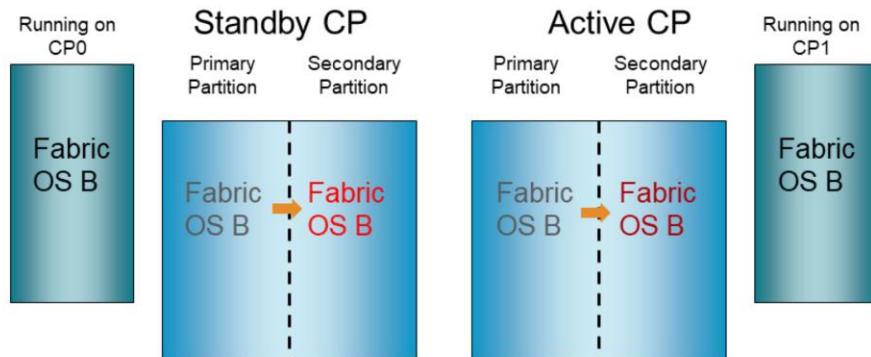
BROCADE
A Broadcom Company

Before the active CP can instruct the standby CP to reboot, the standby CP has to tell the active CP that the checksum is good.

The Standby CP then reboots in order to load the new Fabric OS firmware. At this point both CPs are running the new firmware but it has only been copied to one compact flash. This ensures a level of redundancy, if the upgrade process fails for some reason the switch can revert to the old firmware.

Firmware is Committed on Both CPs

- The last step in the process is to commit the firmware, which copies from each CP Fabric OS B from their Primary Partitions to the Secondary Partitions¹



60 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

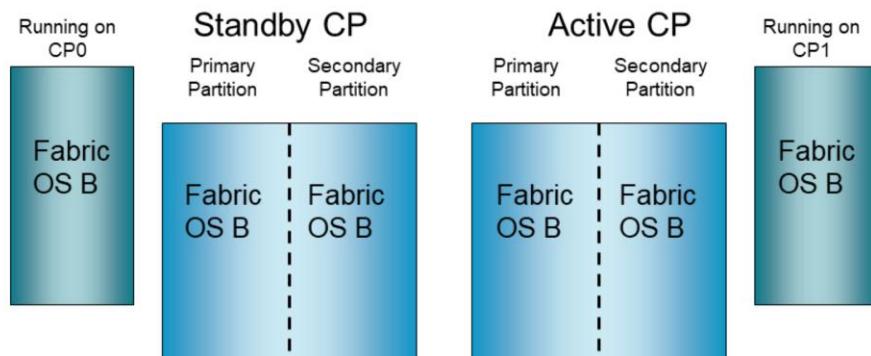
BROCADE
A Broadcom Company

Once both CPs are running the new firmware the Active and Standby CPs perform a firmware commit. This copies the firmware from the primary partition to the secondary compact flash partition.

Firmware Upgrade Completed

- Both CPs running Fabric OS B and all four partitions contain Fabric OS B firmware

Success!



BROCADE
A Broadcom Company

61 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Once the `firmwarecommit` is completed the upgrade process is completed. The new firmware is stored on the primary and secondary partitions of both CP blades, and both CPs are now running the new firmware.

Notice that the CPs have switched roles at the end of the upgrade process. It is possible to revert back to the original Active/Standby roles by issuing the `hashow` command to verify the CPs are in sync and then the `hafailover` command.

Director Switch Firmware Upgrade Example

- Now lets walk through an example: Here the user will upgrade a director from Fabric OS v9.0.0a to Fabric OS v9.0.1b
- Pre-checks, so all partitions have the same firmware versions:

```
X7-4:FID128:admin> firmwareshow
Slot Name      Appl    Primary/Secondary Versions      Status
-----
1  CP0          FOS     v9.0.0a
                     v9.0.0a
2  CP1          FOS     v9.0.0a
                     v9.0.0a
```

62 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Director Switch Firmware Upgrade Example (cont.)

- Checking the status the CPs:

```
X7-4:FID128:admin> hashow
Local CP (Slot 2, CP1): Active, Cold Recovered
Remote CP (Slot 1, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

- In this example notice the following:
 - CP1 is the Active CP
 - CP0 is the Standby CP and is Healthy
 - HA is enabled
 - Heartbeat is Up
 - CP are in Sync (HA State synchronized)
- This director is ready for the firmware upgrade

63 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Director Switch Firmware Upgrade Example (cont.)

- Run the firmwaredownload command from the active CP

```
X7-4:FID128:admin> firmwaredownload  
Server Name or IP Address: 10.124.91.56  
User Name: FW_admin  
File Name: /9.0.1b.G6G7_DIR  
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 2  
Password:
```

Please acknowledge that you have read and accept Broadcom's EULA stipulations.

Please respond (Y/y=accept, N/n=do not accept, or (S/s) to show the EULA) : Y

Checking system settings for firmwaredownload...

System settings check passed.

<continued next slide>

Director Switch Firmware Upgrade Example (cont.)

- Continue with the `firmwareDownload` command:

This command will upgrade the firmware on both CP blades. If you want to upgrade firmware on a single CP only, please use `-s` option.

You may run `firmwareDownloadStatus` to get the status of this command.

This command will cause a warm/non-disruptive boot on the active CP, but will require that existing telnet, secure telnet or SSH sessions be restarted.

```
Do you want to continue (Y/N) [Y]: Y  
Firmware download in progress, please wait.
```

Director Switch Firmware Upgrade Example (cont.)

- Run the `firmwareshow` command to see the status of the partitions

```
X7-4:FID128:admin> firmwareshow
```

Slot Name	Appl	Primary/Secondary Versions	Status
1 CP0	FOS	v9.0.1b Unknown	ACTIVE *
2 CP1	FOS	v9.0.1b v9.0.1b	STANDBY
* Local CP			

Notice this partition
has not yet
completed the
commit¹

- Checking again after a couple of minutes shows the firmware upgrade has completed

```
X7-4:FID128:admin> firmwareshow
```

Slot Name	Appl	Primary/Secondary Versions	Status
1 CP0	FOS	v9.0.1b v9.0.1b	ACTIVE *
2 CP1	FOS	v9.0.1b v9.0.1b	STANDBY
* Local CP			



66 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Footnote 1: If the commit had not yet started it would show the previous version of firmware

Note: See next notes page for an output example from the `firmwaredownloadstatus` command on a director

```
X7-4:FID128:admin> firmwaredownloadstatus
[1]: Tue Aug  5 12:00:12 2021
Slot 2 (CP1, active): Firmware is being downloaded to standby CP.
This step may take up to 30 minutes.

[2]: Tue Aug  5 12:03:28 2021
Slot 2 (CP1, active): Firmware has been downloaded successfully
to Standby CP.

[3]: Tue Aug  5 12:03:28 2021
Slot 2 (CP1, active): Standby CP is going to reboot with new
firmware.

[4]: Tue Aug  5 12:05:05 2021
Slot 1 (CP0, active): Forced failover succeeded. New Active CP is
running new firmware

[5]: Tue Aug  5 12:06:33 2021
Slot 1 (CP0, active): Firmware is being downloaded to standby CP.
This step may take up to 30 minutes.

[6]: Tue Aug  5 12:08:03 2021
Slot 1 (CP0, active): Firmware has been downloaded successfully
on Standby CP.

[7]: Tue Aug  5 12:08:03 2021
Slot 1 (CP0, active): Standby CP reboots.

[8]: Tue Aug  5 12:09:35 2021
Slot 1 (CP0, active): Firmware commit operation has started on
both active and standby CPs.

[9]: Tue Aug  5 12:09:35 2021
Slot 1 (CP0, active): The firmware commit operation has started.
This may take up to 10 minutes.

[10]: Tue Aug  5 12:09:36 2021
Slot 1 (CP0, active): Standby CP booted successfully with new
firmware.

[11]: Tue Aug  5 12:11:51 2021
Slot 1 (CP0, active): The commit operation has completed
successfully.

[12]: Tue Aug  5 12:11:51 2021
Slot 1 (CP0, active): Firmware commit operation has completed
successfully on active CP.

[13]: Tue Aug  5 12:11:51 2021
Slot 1 (CP0, active): Firmwaredownload command has completed
successfully. Use firmwareshow to verify the firmware versions.
```

USB Device Firmware Upgrade



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

USB Storage Device

- Attached the USB drive to a server and copy the unzipped file image to the USB drive
- For a director, only the Active CP is able to mount the USB device, but USB drives can be installed on both CPs
 - Run the `usbstorage -e` command to enable (mount) the USB drive:

```
X7-4:admin> usbstorage -e
```

- Run the `usbstorage -l` command to display the contents of the USB drive

```
X7-4:admin> usbstorage -l
v9.0.0a\ 1126MB 2020 January 30 15:33
Available space on USB storage 96%
```

69 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



All types of USB flash drives are supported in the Brocade Gen 6 and Gen 7 platforms. However, the following USB flash drives are certified by Broadcom:

- SanDisk 32 CZ48 USB 3.0 Flash Drive (SDCZ48-032G-UAM46)
- SanDisk 16 CZ48 USB 3.0 Flash Drive (SDCZ48-016G-UAM46)
- Kingston 32GB DataTraveler 100 G3 USB 3.0 Flash Drive (DT100G3/32GB)
- Kingston 32GB DataTraveler G4 USB 3.0 Flash Drive (DTIG4/32GB)
- PNY Attache 3.0 4 USB 32GB Flash Drive
- PNY Attache 3.0 4 USB 16GB Flash Drive

USB Storage Device (cont.)

- To download firmware from the USB drive run the `firmwaredownload -U` command and provide the firmware file name

```
X7-4:admin> usbstorage -l
v9.0.0a\ 1126MB 2020 January 30 15:33
Available space on USB storage 96%
```

Note: The files sizes will be much smaller with the platform breakout files

```
X7-4:admin> firmwaredownload -U v9.0.0a
Checking system settings for firmware download ...
Protocol selected: USB
<output truncated>
```

70 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



The auto-leveling process automatically ensures compatibility between the version of Fabric OS running on the Active CP and all of the supported AP blades installed in the director chassis. When the Brocade DCX family product boots up or a supported AP blade is inserted or powered on, the Active CP determines if the installed AP blades are running the same version of Fabric OS as the active CP. If the Fabric OS versions differ, the Active CP will install the Fabric OS image on all installed advanced blades. Auto-leveling occurs automatically, without administrator intervention.

Auto-leveling occurs:

- After CP failover (CP error), including during a dual-CP firmware download (e.g. `firmwaredownload -s`)
- After hot-plug of a supported AP blade or when `slotpoweron` is invoked on a slot containing one of these blades
- The active CP always updates the AP blade.
- Auto-leveling is always enabled, and cannot be disabled

Firmware Staging and Testing



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Single-CP Mode

- By default, the `firmwaredownload` command performs a full install including having the auto reboot, and auto commit enabled
- When the `-s` (single CP) option is used (Example: `firmwaredownload -s`) the auto reboot and auto commit modes are configurable, with the autoreboot is OFF by default
 - This results in the firmware be downloaded to the secondary partition only, example:

```
SW1:FID128:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS          v8.2.1c
              v9.0.1b
```

- At this point the firmware is staged (downloaded), but the switch still running on the current (old) Fabric OS (In this example v8.2.1c)

72 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Single-CP Mode (cont.)

- For greater control use the single-CP mode `firmwaredownload -s`, and disable auto-commit and reboot options:

```
SW1:FID128:admin> firmwaredownload -s
Server Name or IP Address: 10.128.91.56
User Name: FW_Admin
File Name: /v9.0.1b.G6_MID
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password:
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]:
Do you accept and agree to the terms outlined in the End User License Agreement
(EULA) for this product?
Please respond with (Y/y) to Accept, (N/n) to Not accept, (D/d) to display the
EULA :y
System settings check passed.
```

In this example the user only wants to stage
(download the firmware), so both the
Auto-commit and reboot options are set to no
(See notes for more information on these options)

Since the upgrade is going
from v8.2.1c to v9.0.1b the
EULA needs to be accepted



73 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

So as we have talked about through out this presentation, when the firmware is downloaded, it gets downloaded into the secondary partition. The reboot option will reboot swap the partition pointers and reboot the switch, so the switch will be running the new firmware. **Setting the Reboot system after download** to no will download the new firmware to the secondary partition but will not reboot the switch. So the switch is still running on the old firmware. This is called staging the firmware, where the switch can be rebooted later to run the new firmware.

If the Auto-Commit option if set to yes, it will copy the firmware from the Active partition to Standby partition after the reboot. If the Do Auto-Commit option is set to no, the old version is kept in the secondary partition, allowing the user to test the new firmware. Giving the user the option to commit the firmware once the testing is complete or restoring the old firmware. More information later in this presentation.

Single-CP Mode (cont.)

- Continuing with the `firmwaredownload -s` command:

You are running `firmwaredownload` with auto-reboot and auto-commit disabled. After the firmware is downloaded, please reboot the system and then run `firmwarecommit` or `firmwarerestore` manually.

Do you want to continue (Y/N) [Y]: **Y**

Firmware is being downloaded to the switch. This step may take up to 30 minutes.
Preparing for `firmwaredownload`...

- Once the firmware downloaded to the Secondary Partition the download process is complete:

```
SW1:FID128:admin> firmwareshow
Appl      Primary/Secondary Versions
```

FOS	v8.2.1c
	v9.0.1b



Single-CP Mode (cont.)

- When ready to run the new firmware just reboot the switch

```
SW1:FID128:admin> reboot
```

- Following the switch reboot, logging back in and running the `firmwareshow` command show the new firmware (v9.0.1b) is in the Primary Partition and is the version currently running on the switch

```
SW1:FID128:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS      v9.0.1b
          v8.2.1c
```

- Now the new firmware can be tested, while still keeping the over version of firmware on the switch

Single-CP Mode (cont.)

- At this point, the user has three options available:
 1. Continue to run the switch with different versions of firmware in each partition
 - This is not recommended for an extended period of time, once the testing phase of the new firmware is complete it is recommended to either commit or restore the firmware
 - Note: Before another firmware download can happen both partitions must be at the same level of firmware (using either the commit or restore options)
 2. Keep the new firmware and run a `firmwarecommit` command which will copy the new firmware to the Secondary Partition
 3. Revert back to the old firmware by running the `firmwarerestore` command
 - This command swaps the partition pointers, so the active partition now contains the old firmware. Then reboots the switch. After the switch reboots, and the switch is now running the old firmware, the old firmware (now in the Active Partition) gets copied to the Secondary Partition. When complete both partitions will contain to the old firmware version

76 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Single-CP Mode (cont.)

- In this example the user choose to keep the new firmware and run the `firmwarecommit` command which copies the firmware from the Primary to the Secondary Partition:

```
SW1:FID128:admin> firmwarecommit
Validating the filesystem ...
Tue Jan  5 17:39:17 2021: Doing firmwarecommit now.
Please wait ...
Tue Jan  5 17:41:23 2021: Firmware commit completed successfully.
```

- Verify the firmware versions in each partition:

```
SW1:FID128:admin> firmwareshow
Appl      Primary/Secondary Versions
-----
FOS          v9.0.1b
              v9.0.1b
```



Firmware History



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Display Firmware History

- To display the firmware history for a switch run the `firmwareshow --history` command:

```
G620:FID128:admin> firmwareshow --history
Firmware version history
```

Sno	Date & Time	Switch Name	Slot	PID	FOS Version
1	Tue Feb 19 16:35:50 2019	unknown(0)	0	1764	Fabos Version 8.2.1a
2	Mon Jul 29 15:27:02 2019	r13-ST03-G620_Edge	0	1782	Fabos Version 8.2.1b
3	Wed Oct 9 16:42:01 2019	G620	0	1981	Fabos Version 8.2.1c
4	Tue Sep 5 16:25:56 2021	G620	0	2354	Fabos Version 9.0.1b

79 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Summary

- In this module we talked about:
 - Brocade Platform Specific firmware image files
 - Brocade Trusted FOS (TruFOS) Certificates
 - Migration paths for FOS v8.2.2c and FOS v9.0.1x
 - How to obtain the firmware from the Broadcom.com web site
 - Fabric OS v9.0.x End User License Agreement (EULA) requirements
 - The firmware upgrade process for both departmental and director switches
 - The staging, testing and committing or restoring firmware on a Brocade switch
- Check the appendix in the PDF for information on:
 - Additional HA commands
 - Obtaining and installing a TruFOS Certificate

80 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.





End of Module:
Brocade Firmware Management Fundamentals
FW-120

Education Services

For more information on Brocade training please contact
brocade.education@broadcom.com

Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Additional HA Commands

- Other commands related to managing high availability include:
 - hasyncstart – Enable HA synchronization
 - hasyncstop – Disable HA synchronization
 - haenable – Enable the HA feature
 - hadisable – Disable the HA feature
 - hafailover – Force a manual CP Card failover from the Active to the Standby CP¹
- Note: These commands are rarely used by most system administrators
 - Do not disable HA unless instructed to do so by an authorized support provider

82 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Footnote 1: The `hareboot` command can also be used and provides the same functionality as the `hafailover` command (Force a manual CP Card failover from the Active CP).

TruFOS Certificate



Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

TruFOS Certificate License ID (LID)

- Brocade X6 and G630 platforms upgraded from any FOS v8.x release to FOS v9.0.0 or v9.0.0a must install a TruFOS certificate¹ prior to migrating to FOS v9.0.1x

- To get the certificate you need the switch license ID, run the command:
license --show -lid

- Example:

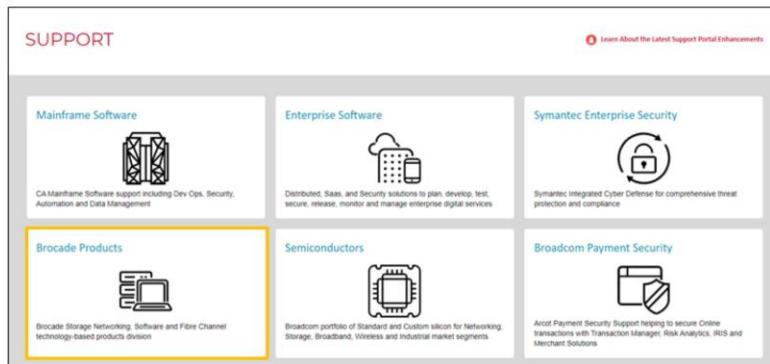
```
SW1:admin> license --show -lid
```

```
10:00:c4:f5:7c:44:1c:cd
```

This is
the LID

TruFOS Certificate Request

- From the website <https://www.broadcom.com>, click **LOGIN**, and enter your username and password, click on **Brocade Products**
 - If you do not have an account, click **REGISTER** to set up your account



85 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE[®]
A Broadcom Company

TruFOS Certificate Request (cont.)

- This brings up the Brocade Products page, scroll down towards the bottom of the page
- Click on **TruFOS Certificate Request**

The screenshot shows a section of the Brocade Products page with several links:

- SAN Reports**: Get an accurate view of your SAN environment, time saving reports, enhanced change tracking, performance graphs and topology diagrams.
- Brocade Support link**: Brocade Support Link
- Training & Education**: Access training and education for Brocade Products
- Knowledge**: Search our Knowledge portal for documentation, configuration guides, and technical details. (Knowledge)
- Education**: All your education needs in one place including our course catalog, fundamentals curriculum path, overview videos and procedures as well as FAQs. (Education)
- Brocade Global Support**: Brocade's complete portfolio of technical support and service offerings to help customers gain operational efficiencies and reduce business risk. (Brocade Global Support)
- TruFOS Certificate Request**: Generate a Trusted FOS certificate. (TruFOS Certificate Request)

86 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE
A Broadcom Company

TruFOS Certificate Request (cont.)

- Enter an email address
- Enter the **License ID** from the switch (see slide 86), or if you have multiple switches you can upload a **file**
 - A file can have up to 100 LIDs listed
 - See notes for information on file format
- When ready, click on the **Submit** button

The screenshot shows a web-based application for requesting TruFOS certificates. At the top, there's a header with 'Input LID' and 'Results'. Below it is a section titled 'Trusted FOS Certificate Request' with a note: 'Please enter 1 to 10 LIDs/WNs. If more than 10 TruFOS Certificates are required, please import a file with up to 100 LIDs/WNs, as described in the Note below. Read [Input Guidelines](#)'. There's an 'Upload File' button highlighted with a yellow box. At the bottom right are 'Submit' and 'Cancel' buttons.

87 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Note: If uploading from a file, supported formats are:

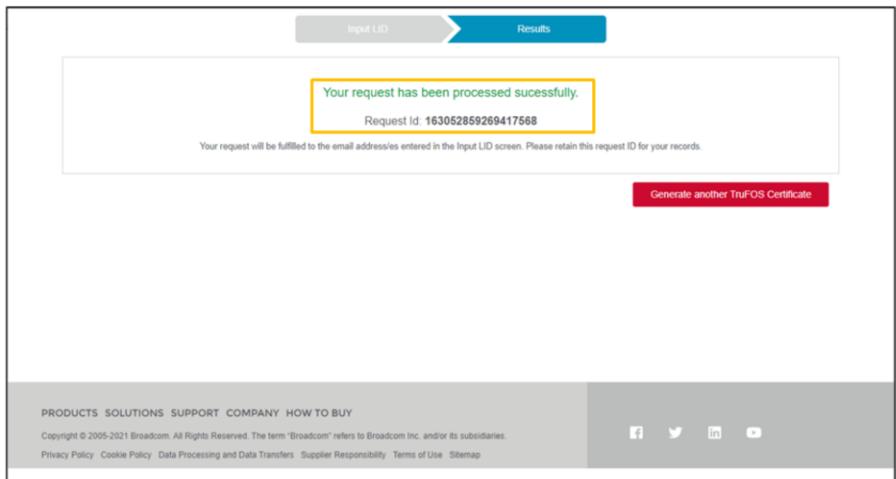
- Use a comma delimited .txt format file such as Wordpad, Notepad and NotePad++. Ensure all LIDs are included in a single comma delimited row with no comma after the final LID. Example:

10:00:c4:f5:7c:41:1e:cc, 10:00:d8:1f:cc:1a:08:a8

- CSV and xls, xlsx, xlsb format Excel files can be imported, with all LIDs sequentially included in the first column (Column A) of the file.

TruFOS Certificate Request (cont.)

- You will get a message that the request has been processed successfully
 - Note the Requested ID, in case the certificate response is not received¹
 - If there were any issues (such as file format was not correct), an error message will be displayed



88 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROCADE[®]
A Broadcom Company

Footnote 1: If the certificate response is not received, contact technical support and they can use the Request ID, to look up the certificate information.

TruFOS Certificate Request (cont.)

- The user will get two emails, the first is a Request ID conformation email, example:

Request ID confirmation email

Dear Sir/Madam,

Our records indicate that you recently requested Trusted FOS certificates. Your request will be fulfilled to the email address/es entered in the Input LID screen. Please save the Request ID below for your future references.

Note: This is an un-monitored mailbox. Do not reply. If you have any issues please reach out to your Contracted Support Organization directly.

Trusted FOS Certificate Request ID: 163052859269417568

Thank you and regards,



89 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

TruFOS Certificate Request (cont.)

- The second email will contain an excel file with the list of submitted LIDs and a zip file which contains the certificate(s)
- Example of the second email:

Dear Sir/Madam,

Our records indicate that you recently requested Trusted FOS Certificates. Here are the details of your transaction.

Please reference the attached excel file for details associated with each LID of your request. The actual Certificates are included within the attached .zip file.

Note: This is an un-monitored mailbox. Do not reply. If you have any issues please reach out to your Contracted Support Organization directly.

Trusted FOS Request ID:	163052559169217568
Requested Date:	2021-09-01 13:36:34.0
Quantity of LIDs Requested:	1

Thank you and regards,



90 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

TruFOS Certificate Installation

- Install the TruFOS certificate on the switch by running the license --install command:

```
SW1:FID128:admin> license --install -h 10.124.91.53 -t scp -u user -p  
passwd -f /download/trufos_certificate.xml
```

- Where:
 - h: provide the IP address for the host
 - t: provide the transport protocol
 - u: provide the user name for the host
 - p: provide the password for host
 - f: provide the path and name filename for the certificate

TruFOS Certificate Installation (cont.)

- Example license --show command output once the TruFOS certificate is loaded onto the switch

```
SW1:FID128:admin> license --show
  License Id : 10:00:c4:f5:7c:2e:c6:91
<truncated output>
License 2 :

-----
  License serial number      : FOS-86-0-04-11203823
  License features          : Trusted FOS (TruFOS) Certificate
  Generation date           : 04/08/2021
  Expiry date               : 04/08/2022
-----
```

92 | Broadcom Proprietary. Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.





This page left intentionally blank