

53-1002274-07
29 December, 2011



Multi-Service IronWare

Software Upgrade Guide R05.2.00c

Supporting Brocade MLX Series and Brocade NetIron Family devices

BROCADE

Copyright © 2006-2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, DCX, Fabric OS, and SAN Health are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

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.

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

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way,
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@Brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@Brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@Brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 - 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@Brocade.com

Document History

Title	Publication number	Summary of changes	Date
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-01	New document	26 July, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-02	Reorganized upgrade content	03 August, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-03	Added new defects for 05.2.00a patch	08 August, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-04	Added new information for 05.2.00b patch	26 September, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-05	Updated hitless upgrade support information	07 October, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-06	Added MR2 upgrade procedure	15 November, 2011
<i>Multi-Service IronWare Software Upgrade Guide</i>	53-1002274-07	Updated FPGA versions	29 December, 2011

Contents

	Audience	vii
	How this document is organized	vii
	Supported hardware	viii
	Document conventions	ix
	Command syntax conventions	ix
	Command examples	ix
	Notes, cautions, and danger notices	ix
	Getting technical help or reporting errors	xi
	Email and telephone access	xi
	Technical support	xi
Chapter 1	Important Upgrade Information for all Supported Devices	
	General upgrade considerations	1
	General downgrade considerations	2
	Special upgrade information for Brocade MLXe devices	2
	FPGA image upgrade information	4
	ifIndex allocation	4
	Upgrade memory requirements	4
Chapter 2	Software upgrades for Brocade MLX Series and Brocade NetIron XMR devices	
	R05.2.00 images	5
	Important memory information for an R05.2.00 upgrade	7
	Clearing code flash memory	7

	Performing a basic upgrade	9
	Basic upgrade Steps	9
	Step 1 - Determining current software image versions.	9
	Step 2 - Upgrading the management module monitor image	12
	Step 3 - Upgrading the management module boot image	12
	Step 4 - Upgrading the combined application image on management modules	13
	Step 5 - Upgrading boot and monitor images on interface modules.	14
	Step 6 - Upgrading interface modules using the combined FPGA image	15
	Step 7 - Performing an image coherence check	16
	Step 8 - Reloading the management module	17
Chapter 3	Brocade MLX Series and Brocade NetIron XMR supplemental upgrade procedures	
	Upgrading MBRIDGE or MBRIDGE32 images on management modules	19
	Upgrading the SBRIDGE image on 32-slot devices	20
	Upgrading the HSBIDGE image on 32-slot devices	20
	Upgrading individual FPGA images on interface modules.	21
Chapter 4	Software Upgrades for Brocade NetIron CER and Brocade NetIron CES devices	
	R05.2.00 images	23
	Performing a basic upgrade	23
	Step 1 - Determining current image versions	24
	Step 2 - Upgrading the application image	25
	Step 3 - Upgrading the fpga-pbif.	25
	Step 4 - Reboot the device	26
	Upgrading monitor and boot images on Brocade NetIron CES and Brocade NetIron CER devices	26

Chapter 5	Software Upgrade for FIPS devices	
	Upgrading Brocade MLXe FIPS devices	27
	FIPS R05.2.00 images for Brocade MLXe devices	27
	Required memory preparation for an	
	R05.2.00 upgrade	29
	Performing a basic upgrade	31
	Basic upgrade steps	32
	Step 1 – Determining current software image versions	32
	Step 2 – Upgrading the management module	
	monitor image	35
	Step 3 – Upgrading the management module	
	boot image	36
	Step 4 – Upgrading the combined application image	
	on management modules	37
	Step 5 – Upgrading boot and monitor images on	
	interface modules	38
	Step 6 – Upgrading interface modules using the	
	combined FPGA image	39
	Step 7 - Performing an image coherence check	40
	Step 8 - Reloading the management module	41
	Supplemental FIPS upgrade procedures for the Brocade MLXe devices	
	42	
	Upgrading Brocade NetIron CES and Brocade NetIron CER	
	FIPS devices	47
	FIPS R05.2.00 images for Brocade NetIron CES and	
	Brocade NetIron CER devices	47
	Step 1 - Determining current image versions	48
	Step 2 - Upgrading the FIPS application image	49
	Step 3 - Upgrading the fpga-pbif	50
	Step 4 - Reload the device	51
	Upgrading monitor and boot images on Brocade NetIron CES and	
	Brocade NetIron CER devices	51
	Downgrading from a FIPS environment to a	
	non-FIPS environment.	52
Chapter 6	Hitless OS Upgrade for all Supported Devices	
	Hitless OS Upgrade support limitations	53
	Special considerations for Hitless OS Upgrade	53
	Hitless OS upgrades for devices running MCT (Multi-Chassis	
	Trunking)	55
	The hitless upgrade process	55
	Performing a hitless upgrade	55
Chapter 7	BR-MLX-MR2 Management Module Upgrade	
Chapter 8	Port and software-based licensing	
	Software license terminology	61

Software-based licensing overview	62
How software-based licensing works	62
Seamless transition for legacy devices	63
License types	63
Licensed features and part numbers	65
Licensing rules	68
Configuration tasks	69
Obtaining a license	69
Installing a license file	73
Verifying the license file installation	74
Using a trial license	74
Viewing information about software licenses	75
Viewing the License ID (LID)	75
Viewing the license database	76
Viewing active packages installed in the device	77
Deleting a license	78
Other licensing options available from the Brocade Software Portal	78
Viewing software license information	78
Transferring a license	80
Special replacement instructions for legacy devices	80
Syslog messages and trap information	81

Chapter 9

Loading and saving configuration files

Brocade MLX Series and Brocade NetIron XMR devices	83
Configuring file size for startup and running configuration	83
Replacing the startup configuration with the running configuration	84
Retaining the current startup configuration	84
Copying a configuration file to or from an SCP or TFTP server	85
Making local copies of the startup configuration file	86
NetIron CES Series and NetIron CER devices	87
Configuring file size for startup and running configuration	87
Replacing the startup configuration with the running configuration	88
Retaining the current startup configuration	88
Copying a configuration file to or from an SCP or TFTP server	88
Making local copies of the startup configuration file	89

Appendix A	Device module considerations	
	Interface module considerations	91
	Upgrading high-speed switch fabric modules	91
Appendix B	Troubleshooting	
	Upgrading devices in MCT topologies	93
	Recovering from a failed upgrade	93
	Troubleshooting a failed FIPS software image installation	95
Appendix C	Patch Upgrade Information for all Supported Devices	
	Required images for R05.2.00c	97
	Brocade MLX Series and Brocade NetIron XMR devices	97
	Brocade NetIron CES and Brocade NetIron CER devices	98
	FIPS R05.2.00c images	99
	Required images for R05.2.00b	101
	Brocade MLX Series and Brocade NetIron XMR devices	101
	Brocade NetIron CES and Brocade NetIron CER devices	102
	FIPS R05.2.00b images	102
	Required images for R05.2.00a	104
	Brocade MLX Series and NetIron XMR devices	104
	Brocade NetIron CES and NetIron Brocade NetIron CER devices	105
	FIPS R05.0.00a images	105

About This Document

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

How this document is organized

This document is organized to help you find information about performing software upgrades for the following devices:

- Brocade MLX Series devices (Brocade MLX and Brocade MLXe)
- Brocade NetIron XMR devices
- Brocade NetIron CER devices
- Brocade NetIron CES devices

The guide contains the following chapters:

- [Chapter 1, “Important Upgrade Information for all Supported Devices”](#) Describes how to find the upgrade information relevant to your devices.
- [Chapter 2, “Software upgrades for Brocade MLX Series and Brocade NetIron XMR devices”](#) Provides upgrade instructions for Brocade MLX Series and Brocade NetIron XMR routers.
- [Chapter 3, “Brocade MLX Series and Brocade NetIron XMR supplemental upgrade procedures”](#) Provides additional upgrade instructions (not covered in the basic upgrade) for Brocade MLX Series and Brocade NetIron XMR routers.
- [Chapter 4, “Software Upgrades for Brocade NetIron CER and Brocade NetIron CES devices”](#) Provides upgrade instructions for Brocade NetIron CER and Brocade NetIron CES devices.
- [Chapter 5, “Software Upgrade for FIPS devices”](#) Provides FIPS upgrade instructions for all devices.
- [Chapter 6, “Hitless OS Upgrade for all Supported Devices”](#) Provides Hitless OS Upgrade instructions.
- [Chapter 7, “BR-MLX-MR2 Management Module Upgrade”](#) Provides instructions to upgrade devices to BR-MLX-MR2 management modules.
- [Chapter 8, “Port and software-based licensing”](#) Provides software-based licensing upgrade instructions for all devices.
- [Chapter 9, “Loading and saving configuration files”](#) Provides instructions on how to load and save configuration files after an upgrade.
- [Appendix A, “Device module considerations”](#) Provides specific interface module requirements.
- [Appendix B, “Troubleshooting”](#) Provides troubleshooting information and additional information about upgrading and installing specific hardware, including management modules, interface modules, switch fabric modules, and fans.

Supported hardware

- [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) lists patch upgrade information for supported devices.

Supported hardware

In instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different hardware configurations are tested and supported by Brocade Communications Systems, Inc., documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are described in this document:

- Brocade MLXe-4 router
- Brocade MLXe-8 router
- Brocade MLXe-16 router
- Brocade MLXe-32 router
- Brocade MLX-4 router
- Brocade MLX-8 router
- Brocade MLX-16 router
- Brocade MLX-32 router
- Brocade NetIron XMR 4000 router
- Brocade NetIron XMR 8000 router
- Brocade NetIron XMR 16000 router
- Brocade NetIron XMR 32000 router
- Brocade NetIron CES 2000 Series
- Brocade NetIron CER 2000 Series

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies document titles
<code>code text</code>	Identifies CLI output

Command syntax conventions

Command syntax in this manual follows these conventions:

command and parameters	Commands and parameters are printed in bold.
[]	Optional parameter.
< <i>variable</i> >	Variables are printed in italics enclosed in angled brackets < >.
...	Repeat the previous element, for example “member [;member...]”
	Choose from one of the parameters.

Command examples

This document describes how to perform simple upgrade and configuration tasks using the command line interface (CLI), but does not describe the commands in detail. For complete descriptions of commands for Brocade MLX Series and Brocade NetIron XMR routers, see the *Brocade MLX Series and Brocade NetIron Family Configuration Guide*.

Notes, cautions, and danger notices

The following notices and danger statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE

A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.



CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Getting technical help or reporting errors

To contact Technical Support, go to <http://www.brocade.com/services-support/index.page> for the latest e-mail and telephone contact information.

Email and telephone access

Go to <http://www.brocade.com/services-support/index.page> for the latest e-mail and telephone contact information.

Technical support

Contact your supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

General information

- Technical Support contract number, if applicable
- Device model
- Operating system version
- Error numbers and messages received
- Detailed description of the problem, including the
- device or network behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Device serial number

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Brocade using one of the following options.

Getting technical help or reporting errors

Important Upgrade Information for all Supported Devices

This chapter contains important information you will need to perform your Multi-Service IronWare software upgrade. Read the following sections carefully before you begin your upgrade process.

For additional up grade information on the following topics, refer to [Appendix B, “Troubleshooting”](#).

- Recovering from a failed upgrade
- Devices in MCT (multi-chassis trunking) topologies

General upgrade considerations

NOTE

The upgrade process for R5.2.00 is different than the previous releases. The upgrade instructions documented here must be followed to upgrade a system from a pre R5.2.00 release to R5.2.00 or higher. If you need assistance with the upgrade process, please contact Brocade Support.

The following general considerations apply to upgrades of Multi-Service IronWare software.

NOTE

Before you begin your R05.2.00 upgrade, you must clear enough code flash memory for the upgrade to be successful. Refer to [“Important memory information for an R05.2.00 upgrade”](#) on page 7.

- **Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules. The following modules support the use of primary and secondary images:**
 - BR-MLX-MR2-X
 - BR-MLX-MR2-M
 - BR-MLX-32-MR2-X
 - BR-MLX-32-MR2-M
 - BR-MLX-10GX2-X
 - NI-MLX-10GX8-D
 - NI-MLX-10GX8-M
 - BR-MLX-10GX8-X
- The combined interface module FPGA image can exceed 32 MB in size, which is greater than the file size limit in older versions of TFTP server applications. Before you use TFTP to transfer image files, be sure that you are using an updated TFTP server capable of handling larger file sizes.
- In most cases boot and monitor images do not need to be upgraded, regardless of whether you are using the combined IronWare image, or are copying images to the management module and interface modules individually. Do not upgrade boot or monitor images unless you are explicitly instructed to do so in the upgrade instructions for the version you are using.

1 General downgrade considerations

- Hitless OS upgrades are *generally* supported for upgrades within a major software release. Hitless OS upgrades are not supported for upgrades from one major release to another major release. For more information about hitless upgrades, refer to [Chapter 6, “Hitless OS Upgrade for all Supported Devices”](#).
- The combined FPGA image is not supported in releases prior to 4.1.00.
- For 32-slot devices, you must copy the SBRIDGE image to each switch fabric module. If you are already running SBRIDGE version 6, this upgrade step is not necessary. Verify your SBRIDGE image using the **show version** command.
- If you are currently running R04.1.00 or 04.1.00a, DO NOT upgrade to SBRIDGE image 6. When loading the SBRIDGE image from a system running 4.1.00 or 4.1.00a, the image on the switch fabric modules may become corrupted. The recommended procedure is to upgrade all images except the SBRIDGE image, reload the device, then upgrade the SBRIDGE image.

General downgrade considerations

The following general considerations apply to downgrades of Multi-Service IronWare software.

- Brocade MLXe routers must not be downgraded to software releases prior to R05.0.00c.
- Brocade MLX and Brocade NetIron XMR 24x1G-X modules (BR-MLX-1GFx24-X-ML, BR-MLX-1GFx24-X, BR-MLX-1GCx24-X-ML, BR-MLX-1GCx24-X) must not be downgraded to versions prior to R05.1.00.
- Brocade MLX and Brocade NetIron XMR 4x10G-X modules (BR-MLX-10Gx4-X, BR-MLX-10Gx4-X-ML) must not be downgraded to versions prior to R05.1.00.
- Brocade MLX 8x10G modules (NI-MLX-10Gx8-M, NI-MLX-10Gx8-D) must not be downgraded to versions prior to R05.0.00b.
- Brocade NetIron XMR 8x10G modules (BR-MLX-10Gx8-X) must not be downgraded to versions prior to R05.2.00.
- Brocade MLX and Brocade NetIron XMR 100G modules (BR-MLX-100Gx2-X, BR-MLX-100Gx1-X) must not be downgraded to versions prior to R05.2.00.
- Brocade MLXe POS interface modules must not be downgraded to versions prior to R03.4.00
- Brocade MLX-32 devices must not be downgraded to versions prior to R03.6.00.
- Brocade NetIron CER devices must not be downgraded to versions prior to R04.1.00a software.
- Brocade MR2 management modules (BR-MLX-Mr2-X and BR-MLX-MR2-M) must not be downgraded to versions prior to R05.2.00b software.

Special upgrade information for Brocade MLXe devices

- Brocade MLXe routers require a minimum software release of R05.0.00c.
- In rare circumstances, you may receive management modules with Brocade MLXe devices that are running R04.0.00b or R04.0.00g.

If your management module is running R04.0.00b, when you boot the device, you will see the following message:

```
"Error: unknown chassis type value 000000f0, system can't come up!"
```

If this occurs, contact Technical Support for guidance on how to upgrade the software.

If your management module is running R04.0.00g, when you boot the device it is recognized as a Brocade NetIron XMR device. Contact Technical support for guidance on how to upgrade the software.

- Although not recommended, if you want to use a management module that has a software image loaded in flash that is older than R05.0.00c in your Brocade MLXe chassis, you must first upgrade the module software to R05.0.00c or later. Contact Technical Support for guidance on how to upgrade the software on this module.

FPGA image upgrade information

NOTE

You must use FPGA images that are specified for Brocade MLX Series or Brocade NetIron XMR devices. If you use FPGA images intended for other products your device will be inoperable.

The following rules apply when upgrading FPGA images on interface modules:

- FPGA images on interface modules must be compatible with the software version running on the router.
- You can upgrade FPGA images individually, or upgrade all FPGA images using the combined FPGA image.
- When you copy the combined FPGA image from to the management module, the management module selects the FPGA images to be downloaded based on the types of interface modules installed and checks for duplicates before downloading the images.
- The FPGA upgrade utility compares the FPGA image version currently installed to new images being downloaded. If the versions are identical, the download is aborted and a warning message is displayed. You can use the force-overwrite option with the FPGA upgrade command to override this feature.
- The bundled FPGA image is more than 32 MB in size. If you are using a TFTP server, be sure that it is capable of handling larger file sizes.

ifIndex allocation

The SNMP Management Information Base (MIB) uses the Interface Index (ifIndex) to assign a unique value to each port on a module or slot. The number of indexes that can be assigned per module is 20, 40, or 64, depending on the number of ports on the module.

For modules with 1 to 20 ports, the ifindex can be set to 20 or 40.

For modules with 24 or more ports, you must set the ifindex to 64 before you install the module. This applies to 48-T interface modules and 1Gx24 copper or fiber interface modules.

To change the ifIndex number, enter the following command at the global config level of the CLI.

snmp-server max-ifindex-per-module 64

For hardware installation instructions, refer to the *Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide*.

Upgrade memory requirements

Before you begin your upgrade, verify that you have enough available bytes free in the flash memory. You should have a minimum of 18 MB available for 32-slot devices, and 16MB for 4, 8, and 16-slot devices to complete your upgrade. To clear enough memory you must first delete existing files. Refer to [“Clearing code flash memory”](#) on page 7.

Software upgrades for Brocade MLX Series and Brocade NetIron XMR devices

This chapter describes how to upgrade your Multi-Service IronWare software to R05.2.00.

NOTE

The software described in this chapter applies only to the Brocade MLX Series and Brocade NetIron XMR devices. You cannot use this software on other Brocade devices.

Before you begin your upgrade, read [Chapter 1, “Important Upgrade Information for all Supported Devices”](#) to make sure your system does not have special upgrade requirements.

R05.2.00 images

NOTE

For all patch releases refer to [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) for the required image names.

The following tables list the images in Multi-Service IronWare R05.2.00.

[Table 1](#) lists the required images for a basic upgrade.

[Table 2](#) lists all images for Multi-Service IronWare R05.2.00.

TABLE 1 Required images for a basic R05.2.00 software upgrade

Image description	Image name
Combined application image for management modules	xm05200.bin
Monitor image for management modules	xmb05200.bin
Monitor image for interface modules	xmlb05200.bin
Boot image for management modules	xmprm05200.bin
Boot image for interface modules	xmlprm05200.bin
Combined FPGA image for interface modules	lpfpga05200.bin

TABLE 2 Multi-Service IronWare R05.2.00 image files

Hardware	Image type	Image name	Compatible version	
Management modules	Boot	xmprm05200.bin	n/a	
	Monitor	xmb05200.bin	n/a	
	Application	xmr05200.bin	n/a	
	Combined application	xm05200.bin	n/a	
	MBRIDGE	mbridge_05200.xsvf	32	
	MBRIDGE32	mbridge32_05200.xsvf (32-slot routers only)	33	
Interface modules	Boot	xmlprm05200.bin	n/a	
	Monitor	xmlb05200.bin	n/a	
	Application	xmlp05200.bin	n/a	
	Combined FPGA	lpfpga05200.bin	n/a	
	Individual FPGA images		pbifsp2_05200.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	3.24
			xppsp2_05200.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	6.23
			xppoc_05200.bin (POS interface modules)	6.22
			pbifoc_05200.bin (POS interface modules)	3.06
			statsoc_05200.bin (POS interface modules)	2.06
			pbifmrj_05200.bin (24x1G and 48x1G modules)	3.25
			xppmrj_05200.bin (24x1G and 48x1G modules)	6.24
			statsmrj_05200.bin (24x1G and 48x1G modules)	0.09
			pbif8x10_05200.bin (8x10G modules)	1.04
			xpp8x10_05200.bin (8x10G modules)	3.08
		xgmacsp2_05200.bin (2x10G and 4x10G modules)	0.15	
		xpp2x100_05200.bin (2x100G modules)	2.20	
	Switch fabric modules	SBRIDGE	sbridge_05200.mcs	6
High speed switch fabric modules	HSBRIDGE	hsbridge_05200.mcs	16	

Performing a patch upgrade

For patch releases, In most cases boot and monitor images do not need to be upgraded. Refer to [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) for information about which images must be upgraded for a specific patch.

Important memory information for an R05.2.00 upgrade

Clearing code flash memory

To provide enough code flash memory to perform the upgrade you must delete the secondary application image files from the active management module. The Multi-Service IronWare software will sync the changes needed to accommodate R05.2.00 to the standby management module during the course of the upgrade process.

NOTE

Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules.

The following modules support the use of primary and secondary images:

BR-MLX-MR2-X

BR-MLX-MR2-M

BR-MLX-32-MR2-X

BR-MLX-32-MR2-M

BR-MLX-10GX2-X

NI-MLX-10GX8-D

NI-MLX-10GX8-M

BR-MLX-10GX8-X

NOTE

You should not need to remove any other files than the ones specified below from the code flash to complete the upgrade.

NOTE

It is recommended that you copy all files to a file server for later retrieval if necessary.

For management modules

To manually delete the secondary files from the *active management module*, perform the following steps:

NOTE

If your set up is not running a secondary image, and you perform these steps, you will receive the following error message:

```
Remove file /flash/secondary failed - File not found
```

1. Delete the secondary application image by entering the following command.
delete secondary
2. Delete the secondary Ip application image by entering the following command.
delete ip-secondary-0
3. Delete any ___**mbridge.old** files from the active management module by entering the following command (three underscores are required in front of **mbridge.old**).
delete ___mbridge.old

2 Important memory information for an R05.2.00 upgrade

4. Enter the **dir** command to check available memory, as shown in this sample output. You should have approximately 18 MB available for 32-slot devices, and approximately 16 MB for 4, 8, and 16-slot devices to complete your upgrade.

```
Brocade# dir
Directory of /flash/
01/11/201103:18:422 $$snmp_boots
09/30/200903:47:505,201 $$sshdsspub.key
06/15/201121:19:04660,145___mbridge
12/07/201022:16:23139 boot parameter
06/15/201121:20:00524,288 lp-monitor-0
06/15/201121:07:444,950,939 lp-primary-0
06/15/201121:19:28524,053 monitor
06/15/201121:08:376,986,237 primary
06/20/201117:11:42620,225 startup-config
9 File(s)14,271,229 bytes
0 Dir(s)16,515,072 bytes free
```

5. Manually delete all unwanted backup configuration files to provide enough memory to accommodate the new images.

For interface modules

To remove secondary application image files from each *interface module*, perform the following steps:

1. Rconsole to each interface module and enter the delete secondary command as shown in this sample output. You should delete the secondary application image file on each interface module.

```
telnet@Router1#rconsole 1
Remote connection to LP slot 1 established
Press CTRL-X or type 'exit' to disconnect it
LP-1>enable
LP-1#delete secondary
LP-1# <ctrl-x>
...
```

2. Enter the **dir** command to check available memory, as shown in this sample output. You should have approximately 8.0 MB per interface module to complete your upgrade.

```
LP-2# dir
Directory of /flash/
File NameSizeChksum
PBIF11281ed
XPP 112 7ff7
boot5242886c2b
monitor524288fd4a
primary4950939df45
5 File(s) 5999739 bytes
Available 58982400 bytes
```

Performing a basic upgrade

The overall procedure for a basic upgrade involves copying only the new application, boot, monitor, and combined FPGA image. If any of the other image versions do not match those listed in [Table 2](#) you will need to upgrade those images as well (for example, individual FPGAs or the MBRIDGE or SBRIDGE images). For instructions on how to upgrade additional images, refer to “[Brocade MLX Series and Brocade Netron XMR supplemental upgrade procedures](#)” on page 19.

Basic upgrade Steps

Please read the full upgrade instructions, listed below, carefully.

Once you have cleared enough code flash memory, you must perform the following steps to complete a basic software upgrade:

- “[Step 1 - Determining current software image versions](#)” on page 9.
- “[Step 2 - Upgrading the management module monitor image](#)” on page 12.
- “[Step 3 - Upgrading the management module boot image](#)” on page 12.
- “[Step 4 - Upgrading the combined application image on management modules](#)” on page 13.
- “[Step 5 - Upgrading boot and monitor images on interface modules](#)” on page 14.
- “[Step 6 - Upgrading interface modules using the combined FPGA image](#)” on page 15.
- “[Step 7 - Performing an image coherence check](#)” on page 16.
- “[Step 8 - Reloading the management module](#)” on page 17.

Step 1 - Determining current software image versions

Before you upgrade your software, you must check the image versions currently installed to determine which ones need to be upgraded (in addition to the images needed for the basic upgrade).

To display image version information, enter the **show flash** or **show version** command. Compare the image versions to the compatible image version numbers in [Table 2](#).

You can view the images stored in flash memory using the **show flash** command.

NOTE

Output examples have been shortened for brevity and do not necessarily reflect all components installed in a system. This example output may not exactly match output from your system.

show flash command output example

In the following examples, the image versions appear in bold.

```
Brocade# show flash
~~~~~
Active Management Module (Left Slot)
Code Flash - Type MT28F128J3, Size 32 MB
o IronWare Image (Primary)
Version 5.1.0T163, Size 6986803 bytes, Check Sum 74d5
Compiled on Mar 16 2011 at 17:49:56 labeled as xmr05100
o IronWare Image (Secondary)
Version 5.1.0T163, Size 6984593 bytes, Check Sum d570
Compiled on Mar 17 2011 at 16:13:36 labeled as xmr05100
```

2 Performing a basic upgrade

```
o LP Kernel Image (Monitor for LP Image Type 0)
Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
Compiled on Mar 11 2011 at 14:07:42 labeled as xmlb05100
o LP IronWare Image (Primary for LP Image Type 0)
Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
Compiled on Mar 16 2011 at 17:55:24 labeled as xmlp05100
o LP IronWare Image (Secondary for LP Image Type 0)
Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
Compiled on Aug 18 2011 at 17:39:16 labeled as xmlp05100
o Monitor Image
Version 5.1.0T165, Size 524053 bytes, Check Sum 70b1
Compiled on Mar 11 2011 at 14:06:30 labeled as xmb05100
o Startup Configuration
Size 12652 bytes, Check Sum dd86
Modified on 21:57:42 Pacific Thu Sep 16 2010
Boot Flash - Type AM29LV040B, Size 512 KB
o Boot Image
Version 5.1.0T165, Size 524038 bytes, Check Sum 59a3
Compiled on Mar 11 2011 at 14:06:58 labeled as xmprm05100
~~~~~
Standby Management Module (Right Slot)
Code Flash: Type MT28F128J3, Size 32 MB
o IronWare Image (Primary)
Version 5.1.0T163, Size 6986803 bytes, Check Sum 74d5
Compiled on Mar 16 2011 at 17:49:56 labeled as xmr05100
o IronWare Image (Secondary)
Version 5.1.0T163, Size 6984593 bytes, Check Sum d570
Compiled on Mar 17 2011 at 16:13:36 labeled as xmr05100
o LP Kernel Image (Monitor for LP Image Type 0)
Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
Compiled on Mar 11 2011 at 14:07:42 labeled as xmlb05100
o LP IronWare Image (Primary for LP Image Type 0)
Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
Compiled on Mar 16 2012 at 17:55:24 labeled as xmlp05100
o LP IronWare Image (Secondary for LP Image Type 0)
Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
Compiled on Mar 18 2011 at 17:39:16 labeled as xmlp05100
o Monitor Image
Version 5.1.0T165, Size 524053 bytes, Check Sum 70b1
Compiled on Mar 11 2011 at 14:06:30 labeled as xmb05100
o Startup Configuration
Size 12652 bytes, Check Sum dd86
Modified on 14:15:27 Pacific Fri Mar 17 2011
Boot Flash: Type AM29LV040B, Size 512 KB
o Boot Image Version 5.1.0T165, Size 524038 bytes, Check Sum 59a3
Compiled on Mar 11 2011 at 14:06:58 labeled as xmprm05100
~~~~~
Line Card Slot 4
Code Flash: Type MT28F640J3, Size 16 MB
o IronWare Image (Primary)
Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
Compiled on Mar 16 2011 at 17:55:24 labeled as xmlp05100
o IronWare Image (Secondary)
Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
Compiled on Mar 18 2011 at 17:39:16 labeled as xmlp05100b1
o Monitor Image
Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
Compiled on Mar 11 2011 at 14:07:42 labeled as xmlb05100
Boot Flash: Type AM29LV040B, Size 512 KB
o Boot Image
```

```
Version 5.1.0T175, Size 492544 bytes, Check Sum 6c2b
Compiled on Mar 11 2011 at 14:07:20 labeled as xmlprm05100
FPGA Version (Stored In Flash):
PBIF Version = 3.24, Build Time = 8/4/2010 14:57:00
XPP Version = 6.03, Build Time = 2/18/2010 16:38:00
STATS Version = 0.08, Build Time = 2/18/2010 16:30:00
```

```
~~~~~
All show flash done
```

show version command output example

```
Brocade# show version
System Mode: MLX
Chassis: Brocade 8-slot (Serial #: GOLD, Part #: 35549-000C)
NI-X-SF Switch Fabric Module 1 (Serial #: PR23050271, Part #: 31523-100A)
FE 1: Type fe200, Version 2
FE 3: Type fe200, Version 2
NI-X-SF Switch Fabric Module 2 (Serial #: SA21091164, Part #: 35523-302A)
FE 1: Type fe200, Version 2
FE 3: Type fe200, Version 2
NI-X-SF Switch Fabric Module 3 (Serial #: SA21091204, Part #: 35523-302A)
FE 1: Type fe200, Version 2
FE 3: Type fe200, Version 2
=====
SL M2: NI-MLX-MR Management Module Active (Serial #: SA21091472, Part #:
35524-103C):
Boot: Version 5.1.0T165 Copyright(c)1996-2011 Brocade Communications Systems, Inc.
Compiled on Feb 11 2011 at 14:06:58 labeled as xmprm05100
(524038 bytes) from boot flash
Monitor: Version 5.1.0T165 Copyright(c)1996-2011 Brocade Communications Systems,
Inc.
Compiled on Feb 11 2011 at 14:06:30 labeled as xmb05100
(524053 bytes) from code flash
IronWare: Version 5.1.0T163 Copyright(c)1996-2011 Brocade Communications Systems,
Inc.
Compiled on Feb 16 2011 at 17:49:56 labeled as xmr05100
(6986803 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 32
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
1024 MB DRAM
Active Management uptime is 1 minutes 28 seconds
=====
SL 4:NI-MLX-1Gx48-T 48-port 10/100/1000Base-T MRJ21 Module(Serial#:
SA05091472,Part#: 35663-20EA)
Boot: Version 5.1.0T175 Copyright(c) 1996-2011 Brocade Communications Systems,
Inc.
Compiled on Feb 11 2011 at 14:07:20 labeled as xmlprm05100
(492544 bytes) from boot flash
Monitor: Version 5.1.0T175 Copyright(c)1996-2011 Brocade Communications Systems,
Inc.
Compiled on Feb 11 2011 at 14:07:42 labeled as xmlb05100
(493244 bytes) from code flash
IronWare: Version 5.1.0T177 Copyright(c)1996-2011 Brocade Communications Systems,
Inc.
Compiled on Feb 16 2011 at 17:55:24 labeled as xmlp05100
(4950936 bytes) from Primary
FPGA versions:
Valid PBIF Version = 3.24, Build Time = 8/4/2010 14:57:00
Valid XPP Version = 6.03, Build Time = 2/18/2010 16:38:00
```

2 Performing a basic upgrade

```
Valid STATS Version = 0.08, Build Time = 2/18/2010 16:30:00
BCM56502GMAC 0
BCM56502GMAC 1
666 MHz MPC 8541 (version 8020/0020) 333 MHz bus
512 KB Boot Flash (AM29LV040B), 16 MB Code Flash (MT28F640J3)
1024 MB DRAM, 8 KB SRAM, 0 Bytes BRAM
PPCR0: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
PPCR1: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
LP Slot 4 uptime is 58 seconds
=====
All show version done
```

You should always check the installed images immediately after an upgrade to confirm that the upgrade was successful.

Step 2 - Upgrading the management module monitor image

To upgrade the monitor image on a management module, perform the following steps:

1. Place the new monitor image on an SCP or TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.
2. Copy the new monitor image to the device by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp xmb<xxxx>.bin <user>@<device-IpAddress>:flash:monitor
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI:
copy tftp flash <tftp-srvr> xmb<xxxx>.bin monitor
- Using the flash card:
copy [slot 1 | slot 2] flash xmb<xxxx>.bin monitor

3. Verify that the new monitor image has been successfully copied by entering the **show flash** command.

Step 3 - Upgrading the management module boot image

To upgrade the boot image on a management module, perform the following steps:

1. Place the new boot image on an SCP or TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.
2. Copy the new boot image to the device by entering one of the following commands.

- Using SCP on a remote client:

```
C:> scp xmprm<xxxx>.bin <user>@<device-IpAddress>:flash:boot
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp flash<tftp-srvr> xmprpm<xxxx>.bin boot
```

- Using the flash card:

```
copy [slot 1 | slot 2] flash xmprpm<xxxx>.bin boot
```

3. Verify that the new boot image has been successfully copied by entering the **show flash** command. Check the image versions, and the date and time when the new images were built.

Step 4 - Upgrading the combined application image on management modules

NOTE

Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules.

The following modules support the use of primary and secondary images:

BR-MLX-MR2-X

BR-MLX-MR2-M

BR-MLX-32-MR2-X

BR-MLX-32-MR2-M

BR-MLX-10GX2-X

NI-MLX-10GX8-D

NI-MLX-10GX8-M

BR-MLX-10GX8-X

1. Place the new software images on an SCP or TFTP server, or on a flash card inserted in slot 1 or 2 on the active management module.
2. Copy the new combined image by entering the following command:
 - Using SCP on a remote client:


```
C:> scp xm<xxxx>.bin <user>@<device-IpAddress>:image: primary
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.
 - Using TFTP at the Privileged EXEC level of the CLI:


```
copy tftp image <tftp-srvr> xm<xxxx>.bin primary
```
 - Using the flash card:


```
copy [slot 1 | slot 2] image xm<xxxx>.bin primary
```
3. Verify that the new image has been successfully copied by entering the **show flash** command at the Privileged Exec level of the CLI and checking the image name and the date and time that it was placed in the directory.

Step 5 - Upgrading boot and monitor images on interface modules

It is recommended that you perform this upgrade from a PC or terminal that is directly connected to the Console port on the management module. You can also perform this procedure through a Telnet or SSHv2 session.

NOTE

Some interface modules require high-speed switch fabric modules and high-speed fans to operate. Refer to [Appendix A, "Device module considerations"](#) for specific upgrade information.

NOTE

If you use the **all** keyword, the LP monitor code is always saved to monitor code space on the management module. If you specify a slot number, the management module copy of the LP code is not changed.

To upgrade monitor and boot images for all interface modules or a specified interface module perform the following steps.

1. Place the new monitor and boot images on an SCP or TFTP server or on a flash card inserted in slot 1 or 2 of the management module.
2. Copy the new monitor and boot images to all interface modules, or to a specified interface module by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp xmlb<xxxx>.bin <user>@<device-IpAddress>:lp:monitor:[all | <slot-number>]
```

```
C:> scp xmlprm<xxxx>.bin <user>@<device-IpAddress>:lp:boot:[all | <slot-number>]
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp lp <tftp-srvr> xmlb<xxxx>.bin monitor [all | <slot-number>]
```

```
copy tftp lp <tftp-srvr> xmlprm<xxxx>.bin boot [all | <slot-number>]
```

- Using the flash card

```
copy [slot 1 | slot 2] lp xmlb<xxx>.bin monitor [all | <slot-number>]
```

```
copy [slot 1 | slot 2] lp xmlprm<xxx>.bin boot [all | <slot-number>]
```

The **all** keyword copies the image to all interface modules.

The *<slot-number>* variable copies the image to a specific interface module.

3. Verify that the new images were successfully copied by entering the **show flash** command. Check the image versions, and the date and time when the new images were built.

Step 6 - Upgrading interface modules using the combined FPGA image

NOTE

The combined interface module FPGA image can exceed 32 MB in size, which is greater than the file size limit in older versions of TFTP server applications. Before you use TFTP to transfer image files, be sure that you are using an updated TFTP server capable of handling larger file sizes.

To upgrade FPGA images on interface modules using the combined FPGA image, perform the following steps:

1. Place the combined FPGA image on an SCP or TFTP server, or on a flash card inserted in management module slot 1 or 2.
2. Copy the combined FPGA image to all interface modules, or to a specific interface module by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp lpfpga<xxxx>.bin <user>@<device-IpAddress> :lp:fgpg-all:[all | <slot-number>]
[:force-overwrite]
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp lp <tftp-srvr> lpfpga<xxxx>.bin fpga-all [<slot-num> | all] [force -overwrite]
```

- Using the flash card:

```
copy [slot 1 | slot 2] lp lpfpga<xxxx>.bin [<slot-num> | all] [force -overwrite]
```

The *<tftp-server>* variable is the address of the TFTP server.

The *<slot-num>* variable specifies the slot number.

The management module compares the copied FPGA versions to the images currently installed on all interface modules (the **all** option), or on a specified interface module (*<slot-number>*). If the FPGA images are identical, the download is aborted and a message appears:

```
Message: Copying 2nd image (PBIF - POS) to slot 1 skipped, same version exists.
Use "force-overwrite" if required.
```

The download continues for interface modules that do not have matching FPGA images.

The **force-overwrite** option allows you to copy the FPGA image identical to the image currently installed. A warning message is not sent. The **force-overwrite** option can also be used for a specific module type.

Step 7 - Performing an image coherence check

When you enter the **reload-check** command, Multi-Service IronWare software performs a coherence check to ensure that compatible versions are installed on management and interface modules, and that all interface module FPGAs are compatible with the current software version. If the software discovers incompatible images, a warning message is sent.

The image coherence check is performed in the following sequence:

1. Check management module and interface module application images for compatibility.
2. Checks the interface module monitor image on the management module and all interface modules.
3. Checks the management module monitor image for compatibility with the management module application image.
4. Checks the interface module monitor image for compatibility the management and interface module application images.
5. Checks all interface module FPGAs for compatibility with the application image. FPGAs include CPP, PBIF, XGMAC, STATS, XPP-OC, PBIF-OC, STATS-OC.

If step 1 does not succeed, verification is stopped and a warning is issued. If step 1 succeeds, the rest of the checks are conducted in parallel.

Performing a coherence check without a reload

Enter the **reload-check** command to perform a coherence check *without* performing a reload.

Example output from this command that shows some inconsistencies is shown here.

```
Brocade# reload-check
Checking for coherence...

Warning: The new LP PBIF-8X10 FPGA will not be compatible with the new LP 3
application.

Warning: The new LP XPP-8X10 FPGA will not be compatible with the new LP 3
application.
Done.
```

Error messages generated by a coherence check

The following error messages are generated if a coherence check fails:

```
Warning: Image coherence check skipped due to insufficient info: Invalid active LP
flash images in Primary/Secondary.
```

```
Warning: Image coherence check skipped due to insufficient info: Invalid active MP
flash images in Primary/Secondary.
```

```
Warning: Image coherence check skipped due to insufficient inf: MP/LP not booting
from flash.
```

```
Warning: Image coherence check skipped due to failure to communicate with LP.
```

If interface modules are in interactive mode, or the system is unable to communicate with the interface modules, the system sends the following warning message:

```
Can't check LP for coherence.
```

Step 8 - Reloading the management module

When you complete your upgrade process, you must reload the management module, which then reboots the interface modules.

To reload the management module, enter one of the following commands:

reload (this command boots from the default boot source, which is the primary code flash)

boot system flash [primary | secondary]

When the management module reboots, the following synchronization events occur:

- The system compares the monitor, primary, and secondary images on a standby management module (if installed) to those on the active management module. If you have updated these images on the active module, the system automatically synchronizes the images on the standby module to match those on the active management module.

If you copied the primary and secondary image to all interface modules using the **copy** command with the **all** keyword, the management module copied the image and stored it in flash memory under the names **lp-primary-0** or **lp-secondary-0**. By default, the system compares the images on the interface modules to the images on the management module to confirm that they are identical. (These images are stored on the management module only and are not run by the management or interface modules.) If the images are not identical, the system gives you the following options.

To replace the images in interface module flash memory with the images in the management module flash memory, enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

To retain the images in the interface module flash memory, enter the **lp cont-boot no-sync <slot-number>** command at the Privileged EXEC prompt.

After the management module finishes booting, perform the following steps.

1. Enter the **show module** command, and verify that the status of all interface modules is **CARD_STATE_UP**.
2. Enter the **show version** command, and verify that all management and interface modules are running the new software image version.

NOTE

If an interface module is in a waiting state or is running an older software image, you may have forgotten to enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

3. If your upgrade fails, for recovery information refer to [Appendix B, “Troubleshooting,”](#) [“Recovering from a failed upgrade”](#) on page 93.
4. Verify that the new images were successfully copied by entering the **show flash** command. Check the image versions, and the date and time when the new images were built.

2 Performing a basic upgrade

Brocade MLX Series and Brocade NetIron XMR supplemental upgrade procedures

The following chapter describe additional upgrade procedures that may be required to upgrade individual images to match those shown in [Table 2](#) on page 6, or upgrades where you are not using the combined FPGA image.

Upgrading MBRIDGE or MBRIDGE32 images on management modules

NOTE

This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to [Table 2](#) on page 6. If your MBRIDGE or MBRIDGE32 image versions differ from those listed, you will need to upgrade them.

To upgrade the MBRIDGE image on your management module, perform the following steps:

NOTE

If you are upgrading a 32-slot device, use the MBRIDGE32 image.

1. Place the new MBRIDGE image on an SCP or TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.
2. Copy the new MBRIDGE image by entering one of the following commands.
 - Using SCP on a remote client:
C:> scp mbridge_<xxx>.xsvf <user>@<device-IpAddress>:mbridge
 - Using TFTP at the Privileged EXEC level of the CLI:
copy tftp mbridge <tftp-srvr> mbridge_<xxx>.xsvf
 - Using the flash card
copy [slot 1 | slot 2] mbridge mbridge_<xxx>.xsvf
3. Verify that the new image has been successfully copied by entering the **show flash** command. Check the image version and the date and time when the new image was built.

Upgrading the SBRIDGE image on 32-slot devices

The SBRIDGE image applies to standard switch fabric modules on 32-slot devices.

NOTE

This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to [Table 2](#) on page 6. If your SBRIDGE image versions differ from those listed in the table, you will need to upgrade them.

To upgrade the SBRIDGE image on switch fabric modules installed in a 32-slot device, perform the following steps:

1. Place the new SBRIDGE image on an SCP or TFTP server, or on a flash card in slot 1 or 2 of the management module.
2. Copy the SBRIDGE image to all switch fabric modules or to a specified switch fabric module by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp sbridge_<xxx>.mcs <user>@<device-IpAddress>:snm:sbridge:[all | <slot-number>]
```

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp snm <tftp-srvr> sbridge_<xxx>.mcs sbridge [all | <slot-number>]
```

- Using the flash card

```
copy [slot 1 | slot 2] snm sbridge_<xxx>.mcs sbridge [all | <slot-number>]
```

The **all** keyword copies the image to all switch fabric modules.

The *<slot-number>* variable copies the image to a specified switch fabric module.

3. Verify that the SBRIDGE image has been successfully copied by entering the **show version** command. Check the image name and the date and time when the new image was built.

Upgrading the HSBRIDGE image on 32-slot devices

The HSBRIDGE image applies to high-speed switch fabric modules installed in 32-slot devices.

NOTE

This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to [Table 1](#) on page 5. If your system image versions differ from those listed in the table, you will need to upgrade them.

To upgrade the HSBRIDGE image on high-speed switch fabric modules installed in a 32-slot device, perform the following steps.

1. Place the new HSBRIDGE image on an SCP or TFTP server, or on a flash card in slot 1 or 2 of the management module.
2. Copy the HSBRIDGE image to all high-speed switch fabric modules or to a specified high-speed switch fabric module by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp hsbridge_<xxxx>.mcs <user>@<device-IpAddress>:snm:sbridge:[all | <snm-index>]
```

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp snm <tftp-srvr> hsbridge_<xxxx>.mcs sbridge [all | <snm-index>]
```

- Using the flash card

```
copy [slot 1 | slot 2] snm hsbridge_<xxxx>.mcs sbridge [all | <snm-index>]
```

The **all** keyword copies the image to all high-speed switch fabric modules.

The *<snm-index>* variable copies the image to a specific high-speed switch fabric module.

3. Verify that the HSBRIDGE image has been successfully copied by entering the **show version** command. Check the image name and the date and time the new image was built.

Upgrading individual FPGA images on interface modules

You can upgrade FPGA images individually on interface modules. To see which individual FPGA images are available, refer to [Table 2](#) on page 6.

NOTE

Brocade recommends using the combined FPGA image to simplify the FPGA image upgrade procedure.

To upgrade FPGA images individually, perform the following steps.

1. Copy each FPGA image from the TFTP server or a flash card to all interface modules, or to a specified interface module by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp <fpga-image-namexxxx.bin> <user>@<device-IpAddress>:lp:[fpga-pbif | fpga-stats | fpga-xgmac | fpga-xpp]:[all | <lp-slot-num>] [:force-overwrite]
```

- Using TFTP at the Privileged EXEC level of the CLI:

```
copy tftp lp <tftp-srvr> <fpga-image-namexxxx.bin> [all | <slot-number> <image-type> <module-type>] [force-overwrite]
```

- Using the PCMCIA flash card

```
copy [slot 1 | slot 2] lp <fpga-image-namexxxx.bin>.bin [all | <module-type>] [force-overwrite]
```

Specify the *<fpga-image-namexxxx.bin>* of the FPGA file you are copying, for example **pbifsp205200.bin**, **xppsp205200.bin**, etc. For a complete list of individual FPGA file names, refer to [Table 2](#) on page 6.

3 Upgrading individual FPGA images on interface modules

If you specify the `<module-type>` the device copies the images for that module only. If you specify **all** without a module-type, the system copies the appropriate images to the corresponding modules.

The system compares FPGA versions being copied to those currently on the interface modules. If the images are identical, the download is aborted, and the following warning message appears.

```
Warning: same version of FPGA already exists on LP, no need to download FPGA again, use force-overwrite option to force download.
```

If you use the **all** option, the system checks each interface module, and sends warning messages for interface modules that have matching FPGA images. For interface modules that do not have matching FPGA images, the software proceeds with the download.

If you use the **force-overwrite** option, an identical image is downloaded and no warning message is sent.

2. The new FPGA images take effect when the management module is rebooted. You can also force the FPGA image to take effect on an interface module without rebooting the management module by “power cycling” the interface module using either of the following methods:
 - Turn the power off and on for the interface module using the **power-off lp <slot-number>** command followed by the **power-on lp <slot-number>** command.
 - Remove and reinsert the interface module.

When the interface module boots, the FPGA Version Check utility confirms that compatible versions of the FPGA images have been installed. At restart or when you enter the **show version** command, the following information appears (the output on your system might vary from this example):

```
Valid PBIF Version = 3.21, Build Time = 03/11/2011 14:44:00
Valid XPP Version = 6.02, Build Time = 02/31/2011 10:52:00
Valid STATS Version = 0.07, Build Time = 01/11/2011 13:33:00
```

If there is a problem with your FPGA upgrade, one of the following warnings will be displayed:

```
WARN: Invalid FPGA version = 1.2, Build Time = 2/13/2011 13:20:0 <<<---
This message indicates an FPGA version mismatch, or that one of the versions is not current:
```

```
ERROR: failed to read FPGA versions from flash <<<---
This message indicates that you have not completed a mandatory FPGA upgrade.
```

Software Upgrades for Brocade NetIron CER and Brocade NetIron CES devices

This chapter describes how to upgrade software on Brocade NetIron CER and Brocade NetIron CES devices. The procedures described are identical for all models, except where indicated.

NOTE

The software described in this section applies only to the Brocade NetIron CER and Brocade NetIron CES devices. You cannot use this software on other Brocade devices.

R05.2.00 images

NOTE

For all patch releases refer to [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) for the required image names.

[Table 3](#) lists the required images and image names for an upgrade to R05.2.00.

TABLE 3 Required images for a basic R05.2.00 software upgrade

Image description	Image name
Application - Multi-Service IronWare	ce05200.bin
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin
fpga-pbif image	pbifmetro_05200.bin

Performing a patch upgrade

For patch releases, in most cases boot and monitor images do not need to be upgraded. Refer to [<cross reference>](#) for information about which images must be upgraded for a specific patch.

Performing a basic upgrade

The following sections describe how to perform a basic software upgrade to R05.2.00.

Before you begin your upgrade, read [Chapter 1, “Important Upgrade Information for all Supported Devices”](#) to make sure your system does not require special upgrade steps.

Upgrading Multi-Service IronWare software for Brocade NetIron CES and Brocade NetIron CER devices usually requires that you upgrade the combined application image only. Boot and monitor images should only be upgraded if you are specifically instructed to do so.

This upgrade requires the following steps:

Step 1 - Determine the image versions currently running on your system. Refer to [“Step 1 - Determining current image versions”](#) on page 24.

4 Performing a basic upgrade

Step 2 - Upgrade the application image. Refer to [“Step 2 - Upgrading the application image”](#) on page 25.

In most cases, these steps are all that is required. If you are directed to upgrade monitor or boot images, follow the procedures described in [“Upgrading monitor and boot images on Brocade NetIron CES and Brocade NetIron CER devices”](#) on page 26.

Step 3 - Upgrade the fpga-pbif on the device. Refer to [“Step 3 - Upgrading the fpga-pbif”](#) on page 25

Step 4 - Reboot the device. Refer to [“Step 4 - Reboot the device”](#) on page 26

Step 1 - Determining current image versions

Before you upgrade the images on a Brocade NetIron CER or Brocade NetIron CES device, you should check the image versions already installed to determine which ones need to be upgraded. You should also check the versions after you complete your upgrade to confirm that the upgrade was successful. Use the **show flash** and **show version** commands to display this information.

Compare the image versions in the output of these commands to the versions listed in [Table 3](#). Upgrade any image versions that do not match those shown in the table.

Examples of output from these commands is shown here.

NOTE

These examples may differ slightly from the information displayed for your system.

show flash command output

```
Brocade# show flash
~~~~~
Code Flash - Type MT28F256J3, Size 64 MB
  o IronWare Image (Primary)
    Version 5.2.0T183, Size 13669945 bytes, Check Sum a4b5
    Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
  o IronWare Image (Secondary)
    Version 5.2.0T183, Size 13669945 bytes, Check Sum a4b5
    Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
  o Monitor Image
    Version 5.1.0T185, Size 445715 bytes, Check Sum 36ab
    Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
  o Startup Configuration
    Size 19267 bytes, Check Sum 663c
    Modified on 15:57:12 Pacific Mon Jun 20 2011

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 5.1.0T185, Size 445715 bytes, Check Sum 36ab
    Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
~~~~~
```

show version command output

```
Brocade#sh version
System: NetIron CER (Serial #: K0SA17F03F, Part #: 40-1000347-04)
License: ADV_SVCS_PREM (LID: mFucGMhFIh)
Boot      : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
(445715 bytes) from boot flash
```

```

Monitor : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
(445715 bytes) from code flash
IronWare : Version 5.2.0T183 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
(13669945 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000d
PBIF: not ready
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 64 MB Code Flash (MT28F256J3)
2048 MB DRAM
Daughter Board: Serial #: L8SA02F056, Part #: 40-1000377-02
System uptime is 34 minutes 53 seconds

```

Step 2 - Upgrading the application image

To upgrade the combined application image (primary or secondary) for Brocade NetIron CER or Brocade NetIron CES devices, perform the following steps:

1. Place the application on an SCP or TFTP server.
2. Copy the new combined image by entering one of the following commands.
 - Using SCP on a remote client:
C:> scp ce<xxx>.bin<user>@<device-IpAddress>:flash:[primary | secondary]
 - Using TFTP at the Privileged EXEC level of the CLI:
copy tftp flash <tftp-srvr> ce<xxx>.bin [primary | secondary]
3. Verify that the new image has been successfully copied by entering the **show flash** command. Check the image version and the date and time the new image was added.

Step 3 - Upgrading the fpga-pbif

To upgrade the fpga-pbif on the Brocade NetIron CER or Brocade NetIron CES device, perform the following steps.

1. Place the pbifmetro_<XXXX>.bin file on a SCP or TFTP server.
2. Copy the fpga-pbif by entering the following commands.
 - Using SCP on a remote client:
C:> scp ce<xxx>.bin<user>@<device-IpAddress>:lp:fpga-pbif:all
 - Using TFTP at the Privileged EXEC Level of the CLI:
copy tftp fpga-pbif <tftp-srvr> pbifmetro_<XXXX>.bin

NOTE

System may take several minutes to finish this procedure, and return control of the console to the user.

Step 4 - Reboot the device

When you complete your upgrade process, you must reboot the device.

1. To reboot the device, enter one of the following commands:
reload (this command boots from the default boot source, which is the primary code flash)
boot system flash [primary | secondary]
2. After the device finishes booting, enter the **show version** command, and verify that the device is running the new software image version.

Upgrading monitor and boot images on Brocade NetIron CES and Brocade NetIron CER devices

In most cases, when upgrading from one major release to another, it is not necessary to upgrade the boot and monitor image for Brocade NetIron CES and Brocade NetIron CER devices, unless you are specifically instructed to do so.

NOTE

Brocade NetIron CER or Brocade NetIron CES devices use the same image for boot and monitor.

To upgrade the monitor and boot image, perform the following steps:

1. Place the new monitor and boot image on an SCP or TFTP server.
2. Copy the new monitor and boot image to the switch using one of the following commands:
 - Using SCP on a remote client:
C:> scp ceb<xxx>.bin <user>@<device-IpAddress>:flash:[boot | monitor]
 - Using TFTP at the Privileged EXEC level of the CLI:
copy tftp flash <tftp-srvr> ceb<xxx>.bin [boot | monitor]
3. Verify that the new monitor and boot images have been successfully copied by entering the show flash command at the Privileged level of the CLI.

If your upgrade fails, for recovery information refer to [Appendix B, “Troubleshooting,”](#) “[Recovering from a failed upgrade](#)” on page 93.

Software Upgrade for FIPS devices

This chapter describes how to perform a FIPS upgrade of Multi-Service IronWare software for the following Brocade devices:

- Brocade MLXe devices - Refer to [“Upgrading Brocade MLXe FIPS devices”](#) on page 27.
- Brocade NetIron CER devices- Refer to [“Upgrading Brocade NetIron CES and Brocade NetIron CER FIPS devices”](#) on page 47.

Upgrading Brocade MLXe FIPS devices

The following sections describe how to upgrade software for Brocade MLXe FIPS devices.

FIPS R05.2.00 images for Brocade MLXe devices

NOTE

For all patch releases refer to [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) for the required image names.

[Table 4](#) lists the minimum required images and signature files to upgrade to R05.2.00. You must have both the image and the signature file to use this upgrade procedure.

[Table 5](#) lists all images and signature files for Multi-Service IronWare R05.2.00.

NOTE

The software described in this section applies only to the Brocade MLXe devices. You cannot use this software on other Brocade devices.

TABLE 4 Required images for a basic upgrade to R05.2.00.

Required image	Image name	Signature file name
Combined application image for management modules	xm05200.bin	xmr05200.sig xmlp05200.sig
Monitor image for management modules	xmb05200.bin	xmb05200.sig
Monitor image for interface modules	xmlb05200.bin	xmlb05200.sig
Boot image for management modules	xmprm05200.bin	xmprm05200.sig
Boot image for interface modules	xmlprm05200.bin	xmlprm05200.sig
Combined FPGA image for interface modules	lfpfga05200.bin	lfpfga05200.sig

5 Upgrading Brocade MLXe FIPS devices

TABLE 5 Multi-Service IronWare R05.2.00 image files

Hardware	Image type	Image name	Signature file name	Compatible version	
Management modules	Boot	xmprm05200.bin	xmprm05200.sig	n/a	
	Monitor	xmb05200.bin	xmb05200.sig	n/a	
	Application	xmr05200.bin	xmr05200.sig	n/a	
	Combined application	xm05200.bin	xmr05200.sig	n/a	
				xmlp05200.sig	n/a
	MBRIDGE MBRIDGE32	mbridge_05200.xsvf mbridge32_05200.xsvf (32-slot routers only)	mbridge_05200.sig mbridge32_05200.sig	32 ^a 33 ^b	
Interface modules	Boot	xmlprm05200.bin	xmlprm05200.sig	n/a	
	Monitor	xmlb05200.bin	xmlb05200.sig	n/a	
	Application	xmlp05200.bin	xmlp05200.sig	n/a	
	Combined FPGA	lpfpga05200.bin	lpfpga05200.sig	n/a	
	Individual FPGA images		pbifsp2_05200.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	pbifsp2_05200.sig	3.24
			xppsp2_05200.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	xppsp2_05200.sig	6.23
			xppoc_05200.bin (POS interface modules)	xppoc_05200.sig	6.22
			pbifoc_05200.bin (POS interface modules)	pbifoc_05200.sig	3.06
			statsoc_05200.bin (POS interface modules)	statsoc_05200.sig	2.06
			pbifmrj_05200.bin (24x1G and 48x1G modules)	pbifmrj_05200.sig	3.25
			xppmrj_05200.bin (24x1G and 48x1G modules)	xppmrj_05200.sig	6.24
			statsmrj_05200.bin (24x1G and 48x1G modules)	statsmrj_05200.sig	0.09
			pbif8x10_05200.bin (8x10G modules)	pbif8x10_05200.sig	1.04
			xpp8x10_05200.bin (8x10G modules)	xpp8x10_05200.sig	3.08
		xgmacsp2_05200.bin (2x10G and 4x10G modules)	xgmacsp2_05200.sig	0.15	
		xpp2x100_05200.bin (2x100G modules)	xpp2x100_05200.sig	2.20	
Switch fabric modules	SBRIDGE	sbridge_05200.mcs	sbridge_05200.sig	6	
High speed switch fabric modules	HSBRIDGE	hsbridge_05200.mcs	hsbridge_05200.sig	16	

a. MR2 management modules use version 36 (for non-32 slot routers); do not downgrade the versions.

b. MR2 management modules use version 35 (for 32-slot routers); do not downgrade the versions.

Performing a patch upgrade

For patch releases, In most cases boot and monitor images do not need to be upgraded. Refer to <cross-reference> for information about which images must be upgraded for a specific patch.

Required memory preparation for an R05.2.00 upgrade

Clearing code flash memory

To provide enough code flash memory to perform the upgrade you must delete the unused application image files from the active management module and from each Ip (primary or secondary). The Multi-Service IronWare software will sync the changes needed to accommodate R05.2.00 to the standby management module during the course of the upgrade process.

The Multi-Service IronWare software does not automatically delete secondary application image files from interface modules. You must manually delete these files before you begin your upgrade.

NOTE

Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules.

The following modules support the use of primary and secondary images:

BR-MLX-MR2-X
 BR-MLX-MR2-M
 BR-MLX-32-MR2-X
 BR-MLX-32-MR2-M
 BR-MLX-100GX2-X
 NI-MLX-10GX8-D
 NI-MLX-10GX8-M
 BR-MLX-10GX8-X

NOTE

You should not need to remove any other files than the ones specified below from the code flash to complete the upgrade.

NOTE

It is recommended that you copy all files to a file server for later retrieval if necessary.

For management modules

To manually delete the secondary files from the *active management module*, perform the following steps:

1. Delete the unused application image by entering the following command:
delete secondary
1. Delete the unused Ip application image by entering the following command:
delete ip-secondary-0
2. Delete any **___mbridge.old** files from the active management module by entering the following command (three underscores are required in front of **mbridge.old**).
delete ___mbridge.old
3. Enter the **dir** command to check available memory, as shown in this sample output. You should approximately 18 MB available for 32-slot devices, and approximately 16 MB for 4, 8, and 16-slot devices to complete your upgrade.

```
Brocade# dir
```

5 Upgrading Brocade MLXe FIPS devices

```
Directory of /flash/
01/11/201103:18:422 $$snmp_boots
09/30/200903:47:505,201 $$sshdsspub.key
06/15/201121:19:04660,145__mbridge
12/07/201022:16:23139 boot parameter
06/15/201121:20:00524,288 lp-monitor-0
06/15/201121:07:444,950,939 lp-primary-0
06/15/201121:19:28524,053 monitor
06/15/201121:08:376,986,237 primary
06/20/201117:11:42620,225 startup-config
9 File(s)14,271,229 bytes
0 Dir(s)16,515,072 bytes free
```

For interface modules

To remove secondary application image files from each *interface module*, perform the following steps:

1. Rconsole to each interface module and enter the delete secondary command as shown in this sample output. You should delete the secondary application image file on each interface module.

```
telnet@Router1#rconsole 1

Remote connection to LP slot 1 established
Press CTRL-X or type 'exit' to disconnect it
LP-1>ena
LP-1#delete secondary
LP-1# <ctrl-x>
...
```

2. Enter the **dir** command to check available memory, as shown in this sample output. You should have approximately 8.0 MB per interface modules to complete your upgrade.

```
LP-2# dir

Directory of /flash/

File NameSizeChksum
PBIF11281ed
XPP 112 7ff7
boot5242886c2b
monitor524288fd4a
primary4950939df45

 5 File(s) 5999739 bytes
 Available 58982400 bytes
```

Performing a basic upgrade

The overall procedure for a basic upgrade involves copying only the new application, boot, monitor, and combined FPGA image. If any of the other image versions do not match those listed in [Table 5](#) you will need to upgrade those images as well (for example, individual FPGAs or the MBRIDGE or SBRIDGE images). For instructions on how to upgrade additional images, refer to [“Supplemental FIPS upgrade procedures for the Brocade MLXe devices”](#) on page 42.

There are two ways to perform an upgrade to FIPS-enabled devices:

- Using Secure Copy (SCP). For more information about SCP, refer to the *Brocade MLX Series and Brocade NetIron Family Configuration Guide*.
- Using a TFTP server. To upgrade Using TFTP at the Privileged EXEC level of the CLI (fips policy allow tftp-access is enabled);, you must first enter the following command in config mode:

```
Brocade(config)# fips policy allow tftp-access
```

Basic upgrade steps

Please read the full upgrade instructions, listed below, carefully.

Once you have cleared enough code flash memory, you must perform the following steps to complete a basic software upgrade:

NOTE

When initially moving from a non-FIPS code base to a FIPS-supported code base, you can use SCP or TFTP and the standard upgrade commands. TFTP can be used with FIPS mode enabled with the proper policy configuration.

- “[Step 1 – Determining current software image versions](#)” on page 32.
 - “[Step 2 – Upgrading the management module monitor image](#)” on page 35.
 - “[Step 3 – Upgrading the management module boot image](#)” on page 36.
 - “[Step 4 – Upgrading the combined application image on management modules](#)” on page 37.
 - “[Step 5 – Upgrading boot and monitor images on interface modules](#)” on page 38.
 - “[Step 6 – Upgrading interface modules using the combined FPGA image](#)” on page 39.
 - “[Step 7 - Performing an image coherence check](#)” on page 40
 - “[Step 8 - Reloading the management module](#)” on page 41.
-

NOTE

When initially moving from a non-FIPS code base to a FIPS supported code base, you can use SCP and can use the standard upgrade commands. TFTP can be used with FIPS mode enabled with the proper policy configuration.

Step 1 – Determining current software image versions

Before you upgrade the software, you should check the image versions currently installed to determine which ones need to be upgraded (in addition to the images needed for the basic upgrade).

To display image version information, enter the **show flash** or **show version** command. Compare the image versions to those shown in [Table 4](#).

Output examples from the **show flash** and **show version** commands are shown here.

NOTE

Output examples have been shortened for brevity and do not necessarily reflect all components installed in a system. This example output may not exactly match output from your system.

show flash command output example

```
Brocade# show flash
~~~~~
Active Management Module (Left Slot)
Code Flash - Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 5.1.0T163, Size 7597514 bytes, Check Sum b4a8
    Compiled on May  9 2011 at 17:55:06 labeled as xmr05100
  o LP Kernel Image (Monitor for LP Image Type 0)
    Version 5.1.0T175, Size 514776 bytes, Check Sum b3b8
    Compiled on May  4 2011 at 16:07:14 labeled as xmlprm05100
```

```

o LP IronWare Image (Primary for LP Image Type 0)
  Version 5.1.0T177, Size 6491775 bytes, Check Sum 49ee
  Compiled on May  9 2011 at 18:01:28 labeled as xmlp05100
o Monitor Image
  Version 5.1.0T165, Size 523278 bytes, Check Sum 98cc
  Compiled on May  4 2011 at 16:06:50 labeled as xmpr05100
o Startup Configuration
  Size 8433 bytes, Check Sum b315
  Modified on 14:08:57 Pacific Tue May 10 2011

Boot Flash - Type AM29LV040B, Size 512 KB
o Boot Image
  Version 5.1.0T165, Size 523293 bytes, Check Sum f0ec
  Compiled on May  4 2011 at 16:06:12 labeled as xmb05100
~~~~~
Standby Management Module (Right Slot)
Code Flash: Type MT28F128J3, Size 32 MB
o IronWare Image (Primary)
  Version 5.1.0T163, Size 7597514 bytes, Check Sum b4a8
  Compiled on May  9 2011 at 17:55:06 labeled as xmr05100
o LP Kernel Image (Monitor for LP Image Type 0)
  Version 5.1.0T175, Size 514776 bytes, Check Sum b3b8
  Compiled on May  4 2011 at 16:07:14 labeled as xmlpr05100
o LP IronWare Image (Primary for LP Image Type 0)
  Version 5.1.0T177, Size 6491775 bytes, Check Sum 49ee
  Compiled on May  9 2011 at 18:01:28 labeled as xmlp05100
o Monitor Image
  Version 5.1.0T165, Size 523278 bytes, Check Sum 98cc
  Compiled on May  4 2011 at 16:06:50 labeled as xmpr05100
o Startup Configuration
  Size 8433 bytes, Check Sum b315
  Modified on 14:08:58 Pacific Tue May 10 2011

Boot Flash: Type MX29LV040C, Size 512 KB
o Boot Image
  Version 5.1.0T165, Size 523293 bytes, Check Sum f0ec
  Compiled on May  4 2011 at 16:06:12 labeled as xmb05100
~~~~~
Line Card Slot 1
Code Flash: Type MT28F256J3, Size 32 MB
o IronWare Image (Primary)
  Version 5.1.0T177, Size 6491775 bytes, Check Sum 49ee
  Compiled on May  9 2011 at 18:01:28 labeled as xmlp05100
o IronWare Image (Secondary)
  Version 5.1.0T177, Size 6277265 bytes, Check Sum 9de9
  Compiled on Dec 13 2010 at 04:30:56 labeled as xmlp05100
o Monitor Image
  Version 5.1.0T175, Size 514776 bytes, Check Sum b3b8
  Compiled on May  4 2011 at 16:07:14 labeled as xmlpr05100
Boot Flash: Type MX29LV040C, Size 512 KB
o Boot Image
  Version 5.1.0T175, Size 515478 bytes, Check Sum 4701
  Compiled on May  4 2011 at 16:07:38 labeled as xmlb05100
FPGA Version (Stored In Flash):
  PBIF Version = 1.04, Build Time = 2/11/2011 10:0:00

XPP Version = 3.08, Build Time = 2/7/2011 10:1:00
.
~~~~~
All show flash done

```

show version command output example

```

Brocade# show version
System Mode: MLX
Chassis: MLXe 8-slot (Serial #: GB2550F03N, Part #: 40-1000362-03)
NI-X-HSF Switch Fabric Module 1 (Serial #: BEU0341F0J0, Part #: 60-1001588-13)
FE 1: Type fe600, Version 1
FE 3: Type fe600, Version 1
NI-X-HSF Switch Fabric Module 2 (Serial #: BEU0338F056, Part #: 60-1001588-13)
FE 1: Type fe600, Version 1
FE 3: Type fe600, Version 1
NI-X-HSF Switch Fabric Module 3 (Serial #: BEU0316F0F4, Part #: 60-1001588-08)
FE 1: Type fe600, Version 1
FE 3: Type fe600, Version 1
=====
SL M1: NI-MLX-MR Management Module Active (Serial #: SA52060253, Part #:
35524-001A):
Boot      : Version 5.1.0T165 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:06:12 labeled as xmb05100
(523293 bytes) from boot flash
Monitor   : Version 5.1.0T165 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:06:50 labeled as xmpr05100
(523278 bytes) from code flash
IronWare  : Version 5.1.0T163 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  9 2011 at 17:55:06 labeled as xmr05100b568
(7597514 bytes) from Primary
Board ID  : 00 MBRIDGE Revision : 32
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
512 MB DRAM INSTALLED
512 MB DRAM ADDRESSABLE
Active Management uptime is 2 days 1 hours 51 minutes 35 seconds
=====
SL M2: NI-MLX-MR Management Module Standby (Serial #: N00450F01R, Part #:
35524-103K):
Boot      : Version 5.1.0T165 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:06:12 labeled as xmb05100
(523293 bytes) from boot flash
Monitor   : Version 5.1.0T165 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:06:50 labeled as xmpr05100
(523278 bytes) from code flash
IronWare  : Version 5.1.0T163 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  9 2011 at 17:55:06 labeled as xmr05100b568
(7597514 bytes) from Primary
Board ID  : 00 MBRIDGE Revision : 32
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (MX29LV040C), 32 MB Code Flash (MT28F128J3)
1024 MB DRAM INSTALLED
1024 MB DRAM ADDRESSABLE
Standby Management uptime is 2 days 1 hours 50 minutes 47 seconds
=====
SL 1: BR-MLX-10Gx8-X 8-port 10GbE (X) Module (Serial #: BQQ0343F00V, Part #:
60-1002154-01)

```

```

Boot      : Version 5.1.0T175 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:07:38 labeled as xmlb05200
(515478 bytes) from boot flash
Monitor   : Version 5.1.0T175 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  4 2011 at 16:07:14 labeled as xmlprm05100
(514776 bytes) from code flash
IronWare  : Version 5.1.0T177 Copyright (c) 1996-2011 Brocade Communications
Systems, Inc.
Compiled on May  9 2011 at 18:01:28 labeled as xmlp05100b568
(6491775 bytes) from Primary
FPGA versions:
Valid PBIF Version = 1.04, Build Time = 2/11/2011 10:0:00

Valid XPP Version = 3.08, Build Time = 2/7/2011 10:1:00

X10G2MAC 0
X10G2MAC 1
X10G2MAC 2
X10G2MAC 3
1333 MHz MPC 8541 (version 8021/0022) 533 MHz bus
512 KB Boot Flash (MX29LV040C), 32 MB Code Flash (MT28F256J3)
2048 MB DRAM, 8 KB SRAM, 0 Bytes BRAM
PPCR0: 0K entries CAM, 0K PRAM, 0K AGE RAM
PPCR1: 0K entries CAM, 0K PRAM, 0K AGE RAM
LP Slot 1 uptime is 5 hours 18 minutes 14 seconds
=====
.
.
.
All show version done

```

You should always check the installed images immediately after an upgrade to confirm that the upgrade was successful.

Step 2 – Upgrading the management module monitor image

To upgrade the monitor image on a management module, perform the following steps:

1. Place the new monitor image on an SCP or TFTP server.
2. Copy the monitor image signature file to the device by entering one of the following commands:
 - Using SCP on a remote client:


```
C:> scp xmb<xxxx>.sig <user>@<device-IpAddress>:flash:monitor.sig
```

The <device-IpAddress> variable is the Ip address of the device where image needs to be transferred.
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):


```
copy tftp flash <tftp-srvr> xmb<xxxx>.sig monitor.sig
```
3. Copy the new monitor image by entering one of the following commands.
 - Using SCP on a remote client:


```
C:> scp xmb<xxxx>.bin <user>@<device-IpAddress>:flash:monitor
```

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled)

```
copy tftp flash <tftp-srvr> xmb<xxxxx>.bin monitor
```

4. Verify that the new monitor image has been successfully copied by entering the **show flash** command.

Step 3 – Upgrading the management module boot image

To upgrade the boot image on a management module, perform the following steps:

1. Place the new boot image on an accessible SCP or TFTP server.
2. Copy the boot image signature file by entering one of the following commands:

- Using SCP on a remote client:

```
C:> scp xmprn<xxxxx>.sig <user>@<device-IPAddress>:flash:boot.sig
```

The *<device-IPAddress>* variable is the IP address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):

```
copy tftp flash <tftp-srvr> xmprn<xxxxx>.sig boot.sig
```

3. Copy the new boot image by entering one of the following commands.

- Using SCP on a remote client:

```
C:> scp xmb<xxxxx>.bin <user>@<device-IPAddress>:flash:boot
```

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):

```
copy tftp flash <tftp-srvr> xmprn<xxxxx>.bin boot
```

4. Verify that the new boot image has been successfully copied by entering the **show flash** command. Check the image versions, and the date and time when the new images were built.

Step 4 – Upgrading the combined application image on management modules

NOTE

Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules.

The following modules support the use of primary and secondary images:

BR-MLX-MR2-X
 BR-MLX-MR2-M
 BR-MLX-32-MR2-X
 BR-MLX-32-MR2-M
 BR-MLX-100GX2-X
 NI-MLX-10GX8-D
 NI-MLX-10GX8-M
 BR-MLX-10GX8-X

1. Place the new software images on an accessible SCP or TFTP server.
2. Back up your running configuration by entering the following command:
 - Using SCP on a remote client:


```
C:\> scp <user>@<device-IpAddress>:runConfig <dst-file>
```
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):


```
copy running-config tftp <tftp-srvr> <dst-file>
```
3. Copy the MP and LP application signature files by entering one of the following commands:

NOTE

You must copy the signature file to the device **before** you copy the binary file.

- Using SCP on a remote client:


```
C:> scp xmr<xxxx>.sig <user>@<device-IpAddress>:flash:primary.sig
```

```
C:> scp xmlp<xxxx>.sig <user>@<device-IpAddress>:flash:lp-pri.sig
```

The *<device-IpAddress>* variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):


```
copy tftp flash <tftp-srvr> xmr<xxxxx>.sig primary.sig
```

```
copy tftp flash <tftp-srvr> xmlp<xxxxx>.sig lp-pri.sig
```
-

NOTE

If the currently running image does not support FIPS, verification against the signature file will not occur.

4. Copy the new combined image from the SCP or TFTP server by entering one of the following commands.
 - Using SCP on a remote client:


```
C:> scp xm<xxxxx>.bin <user>@<device-IpAddress>:image:primary
```

The `<device-IpAddress>` variable is the Ip address of the device where image needs to be transferred.

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):

```
copy tftp image <tftp-srvr> xmlb<xxxxx>.bin [primary | secondary] [delete-first]
```

5. Verify that the new image has been successfully copied by entering the **show flash** command.

Step 5 – Upgrading boot and monitor images on interface modules

To upgrade monitor and boot images for all interface modules or a specified interface module perform the following steps.

1. Place the signature file and new monitor and boot images on an accessible SCP or TFTP server.
2. Copy the boot and monitor image signature files from the SCP or TFTP server by entering one of the following commands:

NOTE

You must copy the signature file to the device **before** you copy the binary file.

- Using SCP on a remote client:

```
C:> scp xmlb<xxxxx>.sig <user>@<device-IpAddress>:flash:lp-mon.sig
```

```
C:> scp xmlprm<xxxxx>.sig <user>@<device-IpAddress>:flash:lp-boot.sig
```

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled)

```
copy tftp flash <tftp-srvr> xmlb<xxxxx>.sig lp-mon.sig
```

```
copy tftp flash <tftp-srvr> xmlprm<xxxxx>.sig lp-boot.sig
```

3. Copy the new monitor and boot images to all interface modules, or to a specified interface module, by entering one of the following commands.

- Using SCP on a remote client:

```
C:> scp xmlprm<xxxxx>.bin <user>@<device-IpAddress>:lp:boot:[all | <slot-number>]
```

```
C:> scp xmlb<xxxxx>.bin <user>@<device-IpAddress>:lp:monitor:[all | <slot-number>]
```

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled)

```
copy tftp lp <tftp-srvr> xmlb<xxxxx>.bin monitor [all | <slot-number>]
```

```
copy tftp lp <tftp-srvr> xmlprm<xxxxx>.bin boot [all | <slot-number>]
```

The **all** keyword copies the image to all modules.

The `<slot number>` variable copies the image to a specified module.

4. Verify that the new images were successfully copied by entering the **show flash** command.

Step 6 – Upgrading interface modules using the combined FPGA image

To upgrade FPGA images on interface modules using the combined FPGA image, perform the following steps:

NOTE

The combined interface module FPGA image can exceed 32 MB in size, which is greater than the file size limit in older versions of SCP server applications. Before you use SCP to transfer image files, be sure that you are using an updated SCP server capable of handling larger file sizes.

1. Place the FPGA signature file and combined FPGA image on an accessible SCP or TFTP server.
2. Copy the FPGA signature file by entering the following command.

NOTE

You must copy the signature file **before** you copy the binary file.

- Using SCP on a remote client:
C:> scp lpfpga<xxxx>.sig <user>@<device-IpAddress>:flash:lpfpga.sig
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> lpfpga<xxxx>.sig lpfpga.sig
3. Copy the combined FPGA image from the SCP or TFTP server to all interface modules, or to a specific interface module by entering one of the following commands:
 - Using SCP on a remote client:
C:> scp lpfpga<xxxx>.bin <user>@<device-IpAddress>:lp:fgpg-all:[all | <slot-number>]:force-overwrite]
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp lp <tftp-srvr> lpfpga<xxxx>.bin fpga-all [<slot-number> | all] [force-overwrite]

The management module compares the copied FPGA versions to the images currently installed on all interface modules (the **all** option), or on a specified interface module (<slot-number>). If the FPGA images are identical, the download is aborted and a message is displayed:

```
Message: Copying 2nd image (PBIF - POS) to slot 1 skipped, same version exists.
Use "force-overwrite" if required.
```

The download continues for interface modules that do not have matching FPGA images.

The **force-overwrite** option allows you to copy the FPGA image identical to the image currently installed. A warning message is not sent. The **force-overwrite** option can also be used for a specific module type.

4. Verify that the new images were successfully copied by entering the **show flash** command.

Step 7 - Performing an image coherence check

When you enter the **reload-check** command, Multi-Service IronWare software performs a coherence check to ensure that compatible versions are installed on management and interface modules, and that all interface module FPGAs are compatible with the current software version. If the software discovers incompatible images, a warning message is sent.

The image coherence check is performed in the following sequence:

1. Check management module and interface module application images for compatibility.
 - a. Checks compatibility of interface module application images on management and interface modules.
 - b. Checks compatibility of interface module monitor images on management and interface modules.
2. Checks interface module monitor image on management module and all interface modules.
3. Checks the management module monitor image for compatibility with the management module application image.
4. Checks the interface module monitor image for compatibility with the management and interface module application images.
5. Checks all interface module FPGAs for compatibility with the application image. FPGAs include CPP, PBIF, XGMAC, STATS, XPP-OC, PBIF-OC, STATS-OC.

If step 1 does not succeed, verification is stopped and a warning is issued. If step 1 succeeds, the rest of the checks are conducted in parallel.

Performing a coherence check without a reload

Enter the **reload-check** command to perform a coherence check *without* performing a reload.

Example output from this command that shows some inconsistencies is shown here.

```
Brocade# reload-check
Checking for coherence...

Warning: The new LP PBIF-8X10 FPGA will not be compatible with the new LP 3
application.

Warning: The new LP XPP-8X10 FPGA will not be compatible with the new LP 3
application.
Done.
```

Error messages generated by a coherence check

The following error messages are generated if a coherence check fails:

```
Warning: Image coherence check skipped due to insufficient info: Invalid active LP
flash images in Primary/Secondary.
```

```
Warning: Image coherence check skipped due to insufficient info: Invalid active MP
flash images in Primary/Secondary.
```

```
Warning: Image coherence check skipped due to insufficient inf: MP/LP not booting
from flash.
```

Warning: Image coherence check skipped due to failure to communicate with LP.

If interface modules are in interactive mode, or the system is unable to communicate with the interface modules, the system sends the following warning message:

```
Can't check LP for coherence.
```

Step 8 - Reloading the management module

When you complete your upgrade process, you must reboot the management module, which then reboots the interface modules.

To reboot the management module, enter one of the following commands:

reload (this command boots from the default boot source, which is the primary code flash)

boot system flash [primary | secondary]

When the management module reboots, the following synchronization events occur:

- The system compares the monitor, primary, and secondary images on a standby management module (if installed) to those on the active management module. If you have updated these images on the active module, the system automatically synchronizes the images on the standby module to match those on the active management module.

If you copied the primary and secondary image to all interface modules using the **copy** command with the **all** keyword, the management module copied the image and stored it in flash memory under the names **lp-primary-0** or **lp-secondary-0** (there will be one or the other, but not both). By default, the system compares the images on the interface modules to the images on the management module to confirm that they are identical. (These images are stored on the management module only and are not run by the management or interface modules.) If the images are not identical, the system gives you the following options.

To replace the images in interface module flash memory with the images in the management module flash memory, enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

To retain the images in the interface module flash memory, enter the **lp cont-boot no-sync <slot-number>** command at the Privileged EXEC prompt.

After the management module finishes booting, perform the following steps.

1. Enter the **show module** command, and verify that the status of all interface modules is **CARD_STATE_UP**.
2. Enter the **show version** command, and verify that all management and interface modules are running the new software image version.

NOTE

If an interface module is in a waiting state or is running an older software image, you may have forgotten to enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

3. If your upgrade fails, for recovery information refer to [Appendix B, "Troubleshooting,"](#) "Recovering from a failed upgrade" on page 93.
4. Verify that the new images were successfully copied by entering the **show flash** command. Check the image versions, and the date and time when the new images were built.

Supplemental FIPS upgrade procedures for the Brocade MLXe devices

This section describes additional upgrade steps you may need to take if your system is running older or incompatible images.

Upgrading MBRIDGE or MBRIDGE32 images on management modules

NOTE

This procedure is generally not required for a major software upgrade. If your router is running old or incompatible image versions you will need to upgrade them.

To upgrade the MBRIDGE image on your management module, perform the following steps:

NOTE

If you are upgrading a 32-slot router, use the MBRIDGE32 image.

1. Place the MBRIDGE signature file and new MBRIDGE image on an accessible SCP or TFTP server.
2. Copy the MBRIDGE signature file from the SCP or TFTP server to the management module by entering one of the following commands.

NOTE

You must copy the signature file to the device **before** you copy the binary file.

- Using SCP on a remote client:
C:> scp mbridge_<xxx>.sig <user>@<device-IpAddress>:flash:mbridge.sig
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> mbridge_<xxx>.sig mbridge.sig
3. Copy the new MBRIDGE image by entering one of the following commands.
 - Using SCP on a remote client:
C:> scp mbridge_<xxx>.xsvf <user>@<device-IpAddress>:mbridge
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp mbridge <tftp-srvr> mbridge_<xxx>.xsvf
 4. Verify that the new image has been successfully copied by entering the **show flash** command.

To upgrade other software images, refer to the appropriate upgrade section.

Upgrading the SBRIDGE image on switch fabric modules for 32-slot devices

NOTE

This procedure is generally not required for a major software upgrade. If your router is running old or incompatible image versions you will need to upgrade them.

To upgrade the SBRIDGE image on switch fabric modules installed in a 32-slot device, perform the following steps:

1. Place the SBRIDGE signature file and new SBRIDGE image on an accessible SCP or TFTP server.
2. Copy the SBRIDGE signature file from the SCP or TFTP server by entering one of the following commands.

NOTE

You must copy the signature file to the device **before** you copy the binary file.

- Using SCP on a remote client:
C:> scp sbridge_<xxxx>.sig <user>@<device-IpAddress>:flash:sbridge.sig
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> sbridge_<xxxx>.sig sbridge.sig
3. Copy the SBRIDGE image from the SCP or TFTP server to all switch fabric modules or to a specified switch fabric module by entering one of the following commands.
 - Using SCP on a remote client:
C:> scp sbridge_<xxxx>.mcs <user>@<device-IpAddress>:snm:sbridge:[all |<slot-number>]
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp snm <tftp-srvr> sbridge_<xxxx>.mcs sbridge [all |<slot-number>]

The **all** keyword copies the image to all switch fabric modules.

The **<slot-number>** variable copies the image to a specified switch fabric module.

4. Verify that the SBRIDGE image has been successfully copied by entering the **show version** command.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module.

Upgrading the HSBRIDGE image on high-speed switch fabric modules for 32-slot devices

NOTE

This procedure is generally not required for a major software upgrade. If your router is running old or incompatible image versions, you will need to upgrade them.

To upgrade the HSBRIDGE image on high-speed switch fabric modules installed in a 32-slot device, perform the following steps:

1. Place the HSBRIDGE signature file and new HSBRIDGE image on an accessible SCP or TFTP server.
2. Copy the HSBRIDGE signature file from the SCP or TFTP server by entering the following command.

NOTE

You must copy the signature file to the device **before** you copy the binary file.

- Using SCP on a remote client:
C:> scp hsbridge_<xxx>.sig <user>@<device-IpAddress>:flash:hsbridge.sig
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> hsbridge_<xxx>.sig hsbridge.sig
3. Copy the HSBRIDGE image from the SCP or TFTP server to all high-speed switch fabric modules or to a specified high-speed switch fabric module by entering one of the following commands:
 - Using SCP on a remote client:
C:> scp hsbridge_<xxx>.mcs <user>@<device-IpAddress>:snm:sbridge:[all |<snm-index>]
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp snm <tftp-srvr> hsbridge_<xxx>.mcs sbridge [all |<snm-index>]

The **all** keyword copies the image to all high-speed switch fabric modules.

The **<snm-index>** variable copies the image to a specific high-speed switch fabric module.
 4. Verify that the HSBRIDGE image has been successfully copied by entering the **show version** command.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module.

Upgrading individual FPGA images on interface modules

Optionally, you can upgrade FPGA images individually on interface modules. To see which FPGA images are available, refer to [Table 5](#).

NOTE

For a simplified FPGA image upgrade process, use the combined FPGA image for interface modules.

To upgrade FPGA images individually, perform the following steps:

1. Copy each FPGA signature file from the SCP or TFTP server by entering one of the following commands:
 - Using SCP on a remote client:


```
C:> scp <fpga-image-namexxxx.sig>
<user>@<device-lpAddress>:flash:<fpga-image-name.sig>
```
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):


```
copy tftp flash <tftp-srvr> fpga <fpga-image-namexxxx.sig> <fpga-image-name>.sig
```
2. Copy each FGPA image file from the SCP or TFTP server by entering one of the following commands:
 - Using SCP on a remote client:


```
C:> scp <fpga-image-namexxxx.bin> <user>@<device-lpAddress>:lp :[fpga-pbif |
fpga-stats | fpga-xgmac | fpga-xpp]:[all | <lp-slot-num>] [:force-overwrite]
```
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):


```
copy tftp lp <tftp-srvr> <fpga-image-namexxxx.bin> [all | <slot-number> [<image-type>
<module-type>] [force-overwrite]
```

Specify the *<fpga-image-name.bin>* variable of the fpga file you are copying, for example, **pbifsp205200.bin**. For a complete list of individual fpga file names, refer to [Table 5](#).

If you specify the *<module-type>*, such as 4x10G, the router copies the images for that module only. If you specify **all** without a module-type, the system copies the appropriate images to the corresponding modules.

The system compares FPGA versions being copied to those currently on the interface modules. If the images are identical, the download is aborted and the following warning message is displayed:

```
Warning: same version of FPGA already exists on LP, no need to download
FPGA again, use force-overwrite option to force download.
```

If you use the **all** option, the system checks each interface module, and sends warning messages for Interface modules that have matching FPGA images. For interface modules that do not have matching FPGA images, the software proceeds with the download.

If you use the **force-overwrite** option, an identical image is downloaded and no warning message sent.

5 Supplemental FIPS upgrade procedures for the Brocade MLXe devices

2. The new FPGA images take effect when the management module is rebooted. You can also force the FPGA image to take effect on an interface module without rebooting the management module by *power cycling* the interface module using either of the following methods:
 - Turn the power off and on for the interface module using the **power-off lp <slot-number>** command followed by the **power-on lp <slot>** command.
 - Remove and reinsert the interface module.

When the interface module boots, the FPGA Version Check utility confirms that compatible versions of the FPGA images have been installed. At restart, or when the **show version** command is entered, the following information is displayed (your version information might vary from what is shown):

```
Valid PBIF Version = 3.21, Build Time = 11/11/2009 14:44:00
Valid XPP Version = 6.02, Build Time = 1/31/2010 10:52:00
Valid STATS Version = 0.07, Build Time = 12/11/2008 13:33:00
```

If there is a problem with your FPGA upgrade, one of the following warnings will be displayed.

```
WARN: Invalid FPGA version = 1.2, Build Time = 9/13/2005 13:20:0 <<<---
```

This message indicates an FPGA version mismatch, or that one of the versions is not current.

```
ERROR: failed to read FPGA versions from flash <<<---
```

This message indicates that you have not completed a mandatory FPGA upgrade.

Upgrading Brocade NetIron CES and Brocade NetIron CER FIPS devices

The following sections describe how to upgrade software for Brocade NetIron CES and Brocade NetIron CER FIPS devices.

FIPS R05.2.00 images for Brocade NetIron CES and Brocade NetIron CER devices

NOTE

For all patch releases refer to [Appendix C, “Patch Upgrade Information for all Supported Devices”](#) for the required image names.

[Table 6](#) lists the minimum required images and signature files to upgrade to R05.2.00. You must have both the image and the signature file to use this upgrade procedure.

NOTE

The software described in this section applies only to the Brocade NetIron CES and Brocade NetIron CER devices. You cannot use this software on other Brocade devices.

TABLE 6 Required images for a FIPS upgrade to R05.2.00.

Required image	Binary image name	Signature Image name	Signature Filename on Flash
Combined application image for management modules - primary	ce05200.bin	ce05200.sig	primary.sig
Combined application image for management modules - secondary	ce05200.bin	ce05200.sig	secondary.sig
Monitor image for management modules	ceb05100.bin	ceb05100.sig	monitor.sig, boot.sig
fpga-pbif image	pbifmetro_05200.bin	pbifmetro_05200.sig	pbifmetro.sig

NOTE

Brocade NetIron CES and Brocade NetIron CER devices use the same file image for boot and monitor images.

There are two ways to perform an upgrade to FIPS-enabled devices:

- Using Secure Copy (SCP). For more information about SCP, refer to the *Brocade MLX Series and Brocade NetIron Family Configuration Guide*.
 - Using a TFTP server. To upgrade Using TFTP at the Privileged EXEC level of the CLI (fips policy allow tftp-access is enabled);, you must first enter the following command in config mode:
fips policy allow tftp-access
-

NOTE

FIPS upgrades using PCMCIA cards are not supported in R05.2.00.

To upgrade your Brocade NetIron CES and Brocade NetIron CER device, perform the following steps:

- [“Step 1 - Determining current image versions”](#) on page 48.
- [“Step 2 - Upgrading the FIPS application image”](#) on page 49.
- [“Step 3 - Upgrading the fpga-pbif”](#) on page 50.
- [“Step 4 - Reload the device”](#) on page 51.

In most cases, unless specifically instructed to do so, you will not need to upgrade the boot and monitor image. If you do need to upgrade this image, refer to [“Upgrading monitor and boot images on Brocade NetIron CES and Brocade NetIron CER devices”](#) on page 51.

Step 1 - Determining current image versions

Before you upgrade your Brocade NetIron CES or Brocade NetIron CER device, you should check the installed image versions to determine which ones need to be upgraded. You should also check the image versions after you complete your upgrade to determine whether the upgrade was successful. You can use the **show flash** and the **show version** commands to display this information.

Examples of output from these commands is shown here.

NOTE

These examples may differ slightly from the information displayed for your system.

show flash command output

```
Brocade# show flash
~~~~~
Code Flash - Type MT28F256J3, Size 64 MB
  o IronWare Image (Primary)
    Version 5.2.0T183, Size 13669945 bytes, Check Sum a4b5
    Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
  o IronWare Image (Secondary)
    Version 5.2.0T183, Size 13669945 bytes, Check Sum a4b5
    Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
  o Monitor Image
    Version 5.1.0T185, Size 445715 bytes, Check Sum 36ab
    Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
  o Startup Configuration
    Size 19267 bytes, Check Sum 663c
    Modified on 15:57:12 Pacific Mon Jun 20 2011

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 5.1.0T185, Size 445715 bytes, Check Sum 36ab
    Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
~~~~~
```

show version command output

```

Brocade#sh version
System: NetIron CER (Serial #: K0SA17F03F, Part #: 40-1000347-04)
License: ADV_SVCS_PREM (LID: mFucGMhFih)
Boot : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
(445715 bytes) from boot flash
Monitor : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Aug 11 2010 at 14:08:06 labeled as ceb05100
(445715 bytes) from code flash
IronWare : Version 5.2.0T183 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Jun 12 2011 at 09:16:48 labeled as ce05200
(13669945 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000d
PBIF: not ready
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 64 MB Code Flash (MT28F256J3)
2048 MB DRAM
Daughter Board: Serial #: L8SA02F056, Part #: 40-1000377-02
System uptime is 34 minutes 53 seconds

```

Step 2 - Upgrading the FIPS application image

For Brocade NetIron CES or Brocade NetIron CER devices, when upgrading from one major release to another, it is usually not necessary to upgrade the boot and monitor images. For R05.2.00, you will need to upgrade the combined application image only.

To upgrade the combined application image on a FIPS-enabled Brocade NetIron CES or Brocade NetIron CER device, perform the following steps.

1. Place the combined application signature file and image on an accessible SCP or TFTP server.

NOTE

If you are Using TFTP at the Privileged EXEC level of the CLI (fips policy allow tftp-access is enabled);, you must first issue the **fips policy allow tftp-access** at the config level.

2. From the SCP or TFTP server, copy the combined application image signature file to the management module by entering one of the following commands.
 - Using SCP on a remote client:

```
C:> scp ce<xxxx>.sig <user>@<device-IpAddress>:flash:[primary.sig | secondary.sig]
```
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):

```
copy tftp flash <tftp-srvr> ce<xxxx>.sig [primary.sig | secondary.sig]
```
3. From the SCP or TFTP server, copy the combined application image file by entering one of the following commands.
 - Using SCP on a remote client:

```
C:> scp ce<xxxx>.bin<user>@<device-IpAddress>:flash:[primary | secondary]
```

- Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):

```
copy tftp flash <tftp-srvr> ce<xxxx>.bin [primary | secondary]
```

NOTE

If the currently running image does not support FIPS, verification against the signature file will not occur.

Step 3 - Upgrading the fpga-pbif

To upgrade the fpga-pbif on the Brocade NetIron CER or Brocade NetIron CES device, perform the following steps.

1. Place the **pbifmetro_<XXXX>.bin** and **pbifmetro_<XXXX>.sig** files on a tftp server.
2. Using SCP or TFTP copy the pbifmetro signature file to the Brocade NetIron CER or Brocade NetIron CES device by entering one of the following commands:
 - Using SCP on a remote client:
C:> scp pbifmetro_<xxxx>.sig <user>@<device-IpAddress>:flash:pbifmetro.sig
 - Using TFTP at the Privileged EXEC level of the CLI (FIPS policy allow tftp-access must be enabled):
copy tftp flash <tftp-srvr> pbifmetro_<xxxx>.sig pbifmetro.sig
3. Copy the **fpga-pbif** image.

NOTE

- FIPS policy allow tftp-access must be enabled.
 - System may take several minutes to finish this procedure, and return control of the console to the user.
-

To copy the **fpga-pbif** image, enter one of the following commands.

- Using SCP on a remote client:
C:> scp pbifmetro_<xxxx>.bin <user>@<device-IpAddress>:lp:fpga-pbif:all
- Using TFTP at the Privileged EXEC Level of the CLI (FIPS policy allow tftp-access must be enabled):
copy tftp fpga-pbif <tftp-srvr> pbifmetro_<xxxx>.bin

Step 4 - Reload the device

When you complete your upgrade process, you must reload the device.

To reload the device, enter one of the following commands:

reload (this command boots from the default boot source, which is the primary code flash)

boot system flash secondary

After the device finishes booting, enter the **show version** command, and verify that the device is running the new software image version.

Upgrading monitor and boot images on Brocade NetIron CES and Brocade NetIron CER devices

In most cases, when upgrading from one major release to another, it is not necessary to upgrade the boot and monitor image for a Brocade NetIron CES or Brocade NetIron CER device, unless you are specifically instructed to do so.

NOTE

Brocade NetIron CES and Brocade NetIron CER devices use the same image for boot and monitor.

To upgrade the monitor and boot image, perform the following steps:

1. Place the new monitor and boot signature file and image on an SCP or TFTP server.
2. From the SCP or TFTP server, copy the monitor and boot image signature file to the Brocade NetIron CES or Brocade NetIron CER device by entering one of the following commands.
 - Using SCP on a remote client:
C:> scp ceb<xxx>.sig <user>@<device-IpAddress>:flash:[monitor.sig | boot.sig]
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> ceb<xxx>.sig [monitor.sig | boot.sig]
3. Copy the new monitor and boot image using one of the following commands:
 - Using SCP on a remote client:
C:> scp ceb<xxx>.bin<user>@<device-IpAddress>:flash:[monitor | boot]
 - Using TFTP at the Privileged EXEC level of the CLI (**fips policy allow tftp-access** must be enabled):
copy tftp flash <tftp-srvr> ceb<xxx>.bin [monitor | boot]
4. Verify that the new monitor and boot images have been successfully copied by entering the **show flash** command at the Privileged level of the CLI.

Downgrading from a FIPS environment to a non-FIPS environment

While a FIPS-supported image is running on the device, at any given time the image can be running in FIPS or non-FIPS mode. In either mode, SSH host-keys are lost because the FIPS supported image saves the host-keys as a file in flash memory, but the downgraded non-FIPS image stores host keys in the backplane EEPROM.

After the device is placed in non-FIPS mode, you can use SCP or TFTP to download and initialize an older image. Use the following steps to revert to a non-FIPS compliant image:

1. Log on to the device by entering your user name and password.
2. Disable FIPS by entering the **no fips enable** command at the prompt.
3. Regenerate ssh host keys or other shared secrets as needed for access after reload.
4. To replace the startup configuration with the **no fips enable** configuration, enter the **write memory** command.

```
Brocade# write memory
```

5. Reload the configuration by entering the **reload** command.

Hitless OS Upgrade for all Supported Devices

This chapter describes the Hitless OS Upgrade feature.

You can upgrade Multi-Service IronWare software using the Hitless OS Upgrade feature with no loss of service or disruption in most functions and protocols. During the hitless upgrade process, all ports and links remain operational.

Hitless OS Upgrade support limitations

Depending on the software version, Hitless OS Upgrade has the following limitations:

- Hitless OS Upgrade is not supported for upgrades between any R05.2.00x releases.

Special considerations for Hitless OS Upgrade

Depending on the software version, Hitless OS Upgrade has the following limitations:

- Both active and standby management modules must be installed to use this feature.
- To avoid disruptions of Layer-3 traffic to OSPF or BGP routes, OSPF Non-stop routing or OSPF Graceful Restart and BGP Graceful Restart features must be configured on the router. In addition, OSPF neighbors of the router must have OSPF Graceful Restart Helper enabled if OSPF Graceful Restart is enabled.
- To avoid disruptions of IPv4 Layer 3 multicast traffic, the unicast routing protocol for multicast RPF routes must be either Non-Stop routing- or Graceful Restart-capable and enabled.
- The time required for the hitless upgrade process ranges from 1 to 10 minutes, depending on the size of the MAC table and the routing table, and the number of OSPF and BGP neighbors. Router configuration is unavailable during the entire hitless upgrade process. The message "--SW Upgrade In Progress - Please Wait--" is displayed at the console if configuration is attempted. Operational command of the router is allowed during the upgrade process.
- Because the active management module becomes the standby management module during the hitless upgrade process, you will need a connection to the console interface on both management modules.
- When they are reset, management and interface modules are unable to send and receive packets. Once the management and interface modules are again operational, modules can send and receive packets, even before the hitless upgrade process is complete.
- Router configuration cannot be changed during the hitless upgrade process.
- Changes to the system-max parameter (or other configuration changes that require a system reload, such as "cam-mode" and "cam-profile" changes) do not take effect after a hitless upgrade.
- FPGA images cannot be upgraded using the hitless upgrade process.
- Hitless upgrade cannot be used to downgrade an image to a version older than the version currently running on the device.
- If there are protocol dependencies between neighboring nodes, it is recommended that you upgrade nodes one at a time.

6 Hitless OS Upgrade for all Supported Devices

- After hitless upgrade, the running configuration on the router will be the same as it was before the upgrade. A configuration that is not saved before a hitless upgrade is not removed and the existing startup configuration does not take effect. This behavior is similar to the management module switchover feature.

]Table 7 lists supported and unsupported protocols and features for Hitless OS Upgrade.

TABLE 7 Supported and unsupported protocols and features for Hitless OS Upgrade

Supported for Hitless OS Upgrade	Not supported for Hitless OS Upgrade
Layer 2 switching	802.1s
Layer 2 protocols:	All MPLS features
MRP	IPv4 and IPv6 multicast snooping
STP	IPv6 multicast routing
RSTP	VLAN translation
VSRP	Policy-based routing
Layer 3 protocols	FPGA upgrades
IGMP	POS
PIM	VRRP and VRRP-E
OSPF	All VPN features
BGP	MCT (Multi-chassis trunking)
IS-IS	Network management to the device:
Static IP routes	SSH
Layer-3 forwarding	Telnet
GRE tunnels	SNTP
ACLs (the following ACLS continue to function but ACL counters are reset)	HTTP/HTTPS
Layer 2 ACLs	sFlow (interface modules only)
IPv4 ACLs	Ping
IPv6 ACLs	Traceroute
IP Receive ACLs	Syslog messages are cleared
IPv4 and Layer-2 ACL-based traffic policing Traffic	SNMP and SNMP trap
policing	DNS
UDLD	DHCP
LACP	AAA
BFD	ERP (G.8032)
802.1ag over VLANs	Management VRF
IPv4 multicast routing	ToS-based QoS

Features not supported for Hitless OS Upgrade may encounter disruptions when the management and interface modules are restarted, but will resume normal operation once the modules become operational.

Hitless OS upgrades for devices running MCT (Multi-Chassis Trunking)

The hitless upgrade process

A hitless upgrade of Multi-Service IronWare software is performed in the following sequence:

1. Multi-Service IronWare software is installed in flash memory to the primary or secondary image on active and standby management modules and interface modules.
2. Enter the **hitless-reload** command on the active management module.
3. The hitless upgrade process starts on the active management module, which initiates the upgrade process on the standby management module.
4. The standby management module is reset.
5. The active management module is reset and the standby management module becomes the active module.
6. Active console control is lost to the previously active management module as it becomes the standby management module.
7. The active management module initiates the upgrade process on all interface modules.
8. The router is now running the new Multi-Service IronWare software. The management module that was initially configured as the standby management module is now the active management module and the management module that was initially configured as the active management module is now the standby management module. If you want the original management module to be active, you must manually fail-over control to it.

Performing a hitless upgrade

NOTE

Hitless upgrades are *generally* supported for upgrades within a major release, but are not supported for upgrades from one major release to another (for example 05.1.xx to 05.2.xx.). Please refer to [“Hitless OS Upgrade support limitations”](#) on page 53 for a list of releases that do not support hitless upgrades.

NOTE

Because of code flash memory considerations, R05.2.00 software operates using a single copy *only* (primary) of each image instead of primary and secondary images on most modules.

The following modules support the use of primary and secondary images:

BR-MLX-MR2-X
 BR-MLX-MR2-M
 BR-MLX-32-MR2-X
 BR-MLX-32-MR2-M
 BR-MLX-100GX2-X
 NI-MLX-10GX8-D
 NI-MLX-10GX8-M
 BR-MLX-10GX8-X

Some features and protocols are not supported for hitless upgrade. Before you perform a hitless upgrade, refer to [Table 7](#) for a list of supported and not-supported features and protocols.

A Hitless OS Upgrade loads from the primary and secondary images on the management modules.

6 Hitless OS Upgrade for all Supported Devices

To perform a Hitless OS Upgrade, use the following procedure:

1. Copy the Multi-Service IronWare software images to the primary or secondary flash on the active and standby management modules and on interface modules.
3. Set up a console connection to both the active and standby management modules. These connections can be serial console sessions or sessions established through Telnet or SSH.
2. Enter the **hitless-reload** command at the console of the active management module.

hitless-reload mp [primary | secondary] | lp [primary | secondary]

The **mp** parameter specifies what image will be loaded from code flash of the *management module*.

The **lp** parameter specifies what image will be loaded from the code flash of the *interface module*.

BR-MLX-MR2 Management Module Upgrade

This chapter describes how to upgrade devices to BR-MLX-MR2 management modules.

The following management modules are referred to as MR:

- NI-MLX-MR
- NI-XMR-MR

The following management modules are referred to as MR2:

- BR-MLX-MR2-X
- BR-MLX-MR2-M

NOTE

The following scenarios are not supported and may result in damage to the MR2 management module and other hardware:

- Installing the MR2 as a standby management module in a device running code prior to NetIron Release 5.2.00b is not supported.
- Installing the MR2 as a standby management module with an MR module in the same device is not supported.
- Installing an MR as a standby module with an MR2 module in the same device is not supported.

If the MR2 module no longer boots, please contact Brocade technical support.

To upgrade to MR2 management modules, perform the following steps:

1. Perform a basic upgrade of your devices to NetIron Release 5.2.00c as documented in the appropriate chapter of this guide for your router.

NOTE

You must complete this step before continuing to the next step.

2. Changes in onboard storage form factors between MR and MR2 management modules require that you back up the configuration while upgrading. Use a TFTP server or SSH client to store the configuration.

To back up the running or startup configurations:

- Using TFTP:

To copy the startup configuration files from the device to a TFTP server, enter the following command:

```
copy startup-config tftp <ip-address> <filename>
```

To copy the running configuration files from the device to an TFTP server, enter the following command:

```
copy running-config tftp <ip-address> <filename>
```

- Using SCP:

To copy the running configuration file on a device to a file on the SCP-enabled host:

```
C:\> scp <user>@<device-IpAddress>:runConfig <dst-file>
```

To copy the startup configuration file on the device to a file on the SCP-enabled client, enter the following command:

```
C:> scp <user>@<device-IpAddress>:startConfig <dst-file>
```

3. Remove the power supplies or power cords to power down the device, and remove the MR management modules. For device specific instructions on removing existing management modules, refer to the appropriate chapter in this document for the device you are using.

NOTE

You should label the network, serial, and power cords to ensure that they are reconnected correctly in [step 4](#) and [step 5](#).

4. Install the MR2 management modules. For device specific instructions on installing management modules, refer to the appropriate chapter in this document for the device you are using. Once the MR2 management modules are correctly installed in the device, reconnect to the serial and network connections.
5. Power the device back on by installing the power supplies or power cords to power on the device.
6. Once the device has come up, connect to the serial port and enter the following commands to assign a temporary IP address to interface m 1, and enable the interface:

```
enable
configure terminal
interface m 1
ip addresss 10.10.10.2/24
enable
exit
ip route 0.0.0.0/0 10.10.10.1
exit
```

NOTE

Adjust the IP addresses and route as needed for your network. You may also need to assign a static route. You should be able to ping the IP address of the TFTP server or SSH client.

7. Copy the startup or running configuration stored from the SSH client or TFTP server back to the device:
 - Using TFTP from the privileged exec mode of the console:

```
copy tftp startup-config <ip-address> <filename>
```

NOTE

SSH is disabled by default, you will need to configure and enable it before using SCP.

- Using SCP:

```
C:> scp <filename> <user>@<device-ipaddress>:config:start
```

NOTE

If your configuration has FIPS mode enabled, you will also need to copy up the needed signature files before reloading. Refer to [Chapter 5, “Software Upgrade for FIPS devices”](#) for information.

8. Issue one of the following commands from the Privileged exec mode of the console to reload the device:

NOTE

You may wish to check that all interface modules are in the up state, and resolve any incompatible versions found before reloading the device.

- To load the primary code flash enter the reload command:

```
reload
```

The **reload** command boots from the default boot source, which is the primary code flash.

- To load the secondary code flash, enter the **boot system flash secondary** command.

```
boot system flash [primary | secondary]
```

After the device has reloaded, verify that everything is working order.

7 BR-MLX-MR2 Management Module Upgrade

Port and software-based licensing

Table 8 lists the individual Brocade NetIron devices and the software licensing features they support.

TABLE 8 Supported software licensing features

Features supported	NetIron XMR Series	NetIron MLX Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_PREM package	CER 2000 Series BASE package	CER 2000 Series Advanced Services package
Software-based licensing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port based-licensing	Yes	Yes	No	No	No	No	No
License generation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
License query	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deleting a license	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Software license terminology

This section defines the key terms used in this chapter.

- **Entitlement certificate** – The proof-of-purchase certificate (*paper-pack*) issued by Brocade when a license is purchased. The certificate contains a unique *transaction key* that is used in conjunction with the *License ID* of the Brocade device to generate and download a software license from the Brocade software portal.
- **License file** – The file produced by the Brocade software portal when the license is generated. The file is uploaded to the Brocade device and controls access to a *licensed feature* or feature set.
- **License ID (LID)** – This is a number that uniquely identifies the Brocade device. The LID is used in conjunction with a *transaction key* to generate and download a software license from the Brocade software portal. The software license is tied to the LID of the Brocade device for which the license was ordered and generated.
- **Licensed feature** – Any hardware or software feature or set of features that require a valid software license in order to operate on the device.
- **Transaction key** – This unique key, along with the *LID*, is used to generate a software license from the Brocade software portal. The transaction key is issued by Brocade when a license is purchased. The transaction key is delivered according to the method specified when the order is placed:

- **Paper-pack** – The transaction key is recorded on an *entitlement certificate*, which is mailed to the customer.
- **Electronic** – The transaction key is contained in an e-mail, which is instantly sent to the customer after the order is placed. The customer will receive the e-mail generally within a few minutes after the order is placed, though the timing will vary depending on the network, internet connection, etc.

If a delivery method was not specified at the time of the order, the key will be delivered via paper-pack.

Software-based licensing overview

Prior to the introduction of software-based licensing, Brocade supported *hardware-based licensing*, where an EEPROM was used to upgrade to a premium set of features. With the introduction of *software-based licensing*, one or more valid software licenses are required to run such *licensed features* on the device.

Software-based licensing is designed to work together with hardware-based licensing. The first release of software-based licensing employs a combination of hardware-based and software-based licensing. A Brocade device can use hardware-based licensing, software-based licensing, or both. Future releases that support software-based licensing will use software-based licensing only, eliminating the need for a customer- or factory-installed EEPROM on the management module or switch backplane.

Software-based licensing provides increased scalability and rapid deployment of hardware and software features on the supported Brocade family of switches. For example, for premium upgrades, it is no longer necessary to physically open the chassis and install an EEPROM to upgrade the system. Instead, the Web is used to generate, download, and install a software license that will enable premium features on the device.

How software-based licensing works

A permanent license can be ordered pre-installed in a Brocade device when first shipped from the factory, or later ordered and installed by the customer. In either case, additional licenses can be ordered as needed.

When a license is ordered separately (not pre-installed), an *entitlement certificate* or e-mail, containing a *transaction key*, are issued to the customer by Brocade as proof of purchase. The *transaction key* and *LID* of the Brocade device are used to generate a license key from the Brocade software licensing portal. The license key is contained within a *license file*, which is downloaded to the customer's PC, where the file can then be transferred to a TFTP or SCP server, then uploaded to the Brocade device.

Once a license is installed on the Brocade device, it has the following effect:

- The license unlocks the licensed feature and it becomes available immediately. There is no need to reload the software.
- When a trial license expires, the commands and CLI related to the feature are disabled, but the feature itself can't be disabled until the system reloads.

Seamless transition for legacy devices

In this chapter, the term **legacy device** refers to a Brocade device that was shipped prior to the introduction of software-based licensing, has an EEPROM installed, and is running pre-release 05.0.00 software.

The transition to software-based licensing is seamless for legacy devices. When upgraded to a release that supports software-based licensing, these devices will continue to operate as previously configured.

Though not mandatory, Brocade recommends that once a legacy device is upgraded to a release that supports software-based licensing, it is also registered. This will enable Brocade to track the device in case service is needed. To register the device, refer to the instructions in [“Special replacement instructions for legacy devices”](#) on page 80.

NOTE

There are special considerations and instructions for legacy NetIron devices in need of replacement (via a Return Merchandise Agreement (RMA)). For details, refer to [“Special replacement instructions for legacy devices”](#) on page 80.

License types

The following license types are supported.

NetIron CES Series license types:

- NI-CES-2024-MEU – Enables Metro Edge Premium upgrade for NetIron CES 2000 Series 24-port models.
- NI-CES-2024-L3U - Enables Layer 3 Premium upgrade for NetIron CES 2000 Series 24-port models.
- NI-CES-2048-MEU – Enables Metro Edge Premium upgrade for NetIron CES 2000 Series 48-port models.
- NI-CES-2048-L3U – Enables Layer 3 Premium upgrade for NetIron CES 2000 Series 48-port models.

Brocade NetIron CER license types:

- NI-CER-2024-ADV – Enables Layer 3 Advanced Premium upgrade for NetIron CER 2000 Series 24-port models.
- NI-CER-2048-ADV – Enables Layer 3 Advanced Premium upgrade for NetIron CER 2000 Series 48-port models.
- NI-CER-2024F-RT - Enables additional memory to support larger routing tables.
- NI-CER-2024C-RT - Enables additional memory to support larger routing tables.
- NI-CER-2024FX-RT - Enables additional memory to support larger routing tables.
- NI-CER-2024CX-RT - Enables additional memory to support larger routing tables.
- NI-CER-2048F-RT - Enables additional memory to support larger routing tables.
- NI-CER-2048C-RT - Enables additional memory to support larger routing tables.
- NI-CER-2048FX-RT - Enables additional memory to support larger routing tables.
- NI-CER-2048CX-RT - Enables additional memory to support larger routing tables.

Brocade MLX Series and NetIron XMR license Types:

8 Software-based licensing overview

- BR-MLX-10GX4-X - Enables License upgrade to NetIron MLX and Brocade MLXe 4-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support - requires XFP optics. Supports 1 million IPv4 routes in FIB.
 - BR-MLX-1GCx24-X - Enables 24-port 1Gbps copper module for wire-speed performance.
 - BR-MLX-1GFx24-X - Enables 24-port 1Gbps fiber module for wire-speed performance.
 - BR-MLX-100GX1-2PUPG - Enables 100 GbE second port license upgrade —requires CFP optics.
-
- **Trial license** – Also called a **temporary license**, this enables a license-controlled feature to run on the device on a temporary basis. A trial license enables demonstration and evaluation of a licensed feature and can be valid for a period of 45 days. For more information about a trial license, see [“Using a trial license”](#) on page 74.
 - **Normal license** – Also called a **permanent license**, this enables a license-controlled feature to run on the device indefinitely.

Licensed features and part numbers

Table 9 lists the supported licensed features, associated image filenames, and related part numbers.

NOTE

There are no changes to the part numbers for products with pre-installed (factory-installed) licenses. These part numbers are listed for reference in the last column of Table 9.

TABLE 9 Licensed features and part numbers for the Netron CES and Netron CER devices

Product	Licensed feature or feature set	Image filename	Part numbers for software license only	Part numbers for hardware with pre-installed software license
Netron CES	EPREM Metro Edge Premium (Metro Edge Premium License) <ul style="list-style-type: none"> • All Classic Layer 2 capabilities • Base Layer 3 (RIP and static routes) • QoS and ACLs • Management via SNMP and CLI • IP over MPLS (IGP shortcuts) • GRE • Policy Based Routing (PBR) • Provider Bridges (IEEE 802.1ad) • Provider Backbone Bridges (IEEE 802.1ah) • In-band management for PB/PBB network • OSPF and ISIS • Connectivity Fault Management (IEEE 802.1ag) and Service OAM • Ethernet Service Instance (ESI) framework • Multi-VRF • MPLS (VPLS, VLL) • 802.3ah Link OAM • Static IPv6 • RIPng • OSPFv3 • IS-ISv6 	cerxxxxx.bin	<ul style="list-style-type: none"> • 24 ports: NI-CES-2024-MEU 	NI-CES-2024F-MEPREM-AC NI-CES-2024F-MEPREM-DC NI-CES-2024C-MEPREM-AC NI-CES-2024C-MEPREM-DC NI-CES-2024FX-MEPREM-AC NI-CES-2024FX-MEPREM-DC NI-CES-2024CX-MEPREM-AC NI-CES-2024CX-MEPREM-DC
			<ul style="list-style-type: none"> • 48 ports: NI-CES-2048-MEU 	NI-CES-2048F-MEPREM-AC NI-CES-2048F-MEPREM-DC NI-CES-2048C-MEPREM-AC NI-CES-2048C-MEPREM-DCNI NI-CES-2048FX-MEPREM-AC NI-CES-2048FX-MEPREM-DC NI-CES-2048CX-MEPREM-AC NI-CES-2048CX-MEPREM-DC

TABLE 9 Licensed features and part numbers for the Netron CES and Netron CER devices (Continued)

Product	Licensed feature or feature set	Image filename	Part numbers for software license only	Part numbers for hardware with pre-installed software license
	EPREM L3_PREM (Layer 3 Premium License) <ul style="list-style-type: none"> • All Classic Layer 2 capabilities • Base Layer 3 (RIP and static routes) • QoS and ACLs • Management via SNMP and CLI • Full Layer 3 capabilities, including OSPF, ISIS, and BGP • Multi-VRF • Static IPv6 • RIPng • IS-ISv3 • OSPFv3 • BGP shortcuts (requires L3_PREM and ME_PREM) • GRE • Policy Based Routing (PBR) 	cerxxxxx.bin	<ul style="list-style-type: none"> • 24 ports: NI-CES-2024-L3U • 48 ports: NI-CES-2048-L3U 	NI-CES-2024F-L3PREM-AC NI-CES-2024F-L3PREM-DC NI-CES-2024C-L3PREM-AC NI-CES-2024C-L3PREM-DC NI-CES-2024FX-L3PREM-AC NI-CES-2024FX-L3PREM-DC NI-CES-2024CX-L3PREM-AC NI-CES-2024CX-L3PREM-DC NI-CES-2048F-L3PREM-AC NI-CES-2048F-L3PREM-DC NI-CES-2048C-L3PREM-AC NI-CES-2048C-L3PREM-DC NI-CES-2048FX-L3PREM-AC NI-CES-2048FX-L3PREM-DC NI-CES-2048CX-L3PREM-AC NI-CES-2048CX-L3PREM-DC

TABLE 9 Licensed features and part numbers for the Netron CES and Netron CER devices (Continued)

Product	Licensed feature or feature set	Image filename	Part numbers for software license only	Part numbers for hardware with pre-installed software license
Netron CER	Advanced Services Premium:	cerxxxxx.bin	<ul style="list-style-type: none"> 24 ports: NI-CER-2024-ADV 	NI-CER-2024F-ADVPREM-AC NI-CER-2024F-ADVPREM-DC NI-CER-2024C-ADVPREM-AC NI-CER-2024C-ADVPREM-DC NI-CER-2024FX-ADVPREM-AC NI-CER-2024FX-ADVPREM-DC NI-CER-2024CX-ADVPREM-AC NI-CER-2024CX-ADVPREM-DC
	<ul style="list-style-type: none"> Full Layer 3, including RIP, OSPF, IS-IS, and BGP Virtual routing in non-MPLS environments via Multi-VRF All classic Layer 2 capabilities QoS and ACLs Management via SNMP/CLI Multi-Protocol Label Switching (MPLS) Layer 2 VPNs using VPLS and VLLs Provider Bridges (IEEE 802.1ad) Provider Backbone Bridges (IEEE 802.1ah) Connectivity Fault Management (IEEE 802.1ag) and Service OAM Ethernet Service Instance (ESI) framework 		<ul style="list-style-type: none"> 48 ports: NI-CER-2048-ADV 	NI-CER-2048F-ADVPREM-AC NI-CER-2048F-ADVPREM-DC NI-CER-2048C-ADVPREM-AC NI-CER-2048C-ADVPREM-DC NI-CER-2048FX-ADVPREM-AC NI-CER-2048FX-ADVPREM-DC NI-CER-2048CX-ADVPREM-AC NI-CER-2048CX-ADVPREM-DC
	CER-RT: Adds additional memory to support larger routing tables.	cerxxxxx.bin	IP_ROUTE_SCALE	NI-CER-2024F-RT-AC NI-CER-2024F-RT-DC NI-CER-2024C-RT-AC NI-CER-2024C-RT-DC NI-CER-2024FX-RT-AC NI-CER-2024FX-RT-DC NI-CER-2024CX-RT-AC NI-CER-2024CX-RT-DC NI-CER-2048F-RT-AC NI-CER-2048F-RT-DC NI-CER-2048C-RT-AC NI-CER-2048C-RT-DC NI-CER-2048FX-RT-AC NI-CER-2048FX-RT-DC NI-CER-2048CX-RT-AC NI-CER-2048CX-RT-DC

TABLE 10 Brocade MLX Series and Brocade NetIron Family routers

Product	Licensed feature or feature set	Image filename	Part numbers for software license only	Part numbers for hardware with pre-installed software license
Brocade MLX Series and Brocade NetIron XMR routers	10x4G license upgrade (Brocade MLX and Brocade MLXe):	xgmacsp2_05200.bin	BR-MLX-10GX4-XUPG	BR-MLX-10GX4-X
	<ul style="list-style-type: none"> 4-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support - requires XFP optics. Supports 1 million IPv4 routes. 			
	100 GbE second port license upgrade:	xpp2x100.bin	BR-MLX-100GX1-2PUPG	BR-MLX-100GX2-X
	<ul style="list-style-type: none"> Brocade MLX Series 100 GbE second port license upgrade —requires CFP optics. 			
24x1G Copper license upgrade:	<ul style="list-style-type: none"> Enables 24-port 1Gbps copper module for wire-speed performance 	pbifmrj_05200.bin	BR-MLX-1Gx4-UPG	BR-MLX-1GCx24-X
		xppmrj_05200.bin statsmrj_05200.bin		
24x1G Fiber license upgrade:	<ul style="list-style-type: none"> Enables 24-port 1Gbps fiber module for wire-speed performance. 	pbifmrj_05200.bin	BR-MLX-1Gx4-UPG	BR-MLX-1GFx24-X
		xppmrj_05200.bin statsmrj_05200.bin		

Licensing rules

This section lists the software licensing rules and caveats related to the Brocade devices that support software-based licensing.

General notes

The following licensing rules apply to all NetIron devices that support software licensing:

- A license is tied to the unique LID of the fixed configuration switch for which the license was ordered. Therefore, a license can be used on one particular device only. It cannot be used on any other device.
- More than one license can be installed per device concurrently.

- More than one trial license can be in effect at the same time, as long as each trial license applies to a unique licensed feature.
- A trial license cannot replace or supersede a normal license.

Configuration tasks

This section describes the configuration tasks for generating and obtaining a software license, then installing it on the Brocade device. Perform the tasks in the order listed in [Table 11](#).

TABLE 11 Configuration tasks for software licensing

Configuration task	See...
1 Order the desired license.	For a list of available licenses and associated part numbers, see “Licensed features and part numbers” on page 65.
2 When you receive the transaction key, retrieve the LID of the Brocade device. If you received the transaction key via paper-pack, record the LID on the entitlement certificate in the space provided.	“Viewing the License ID (LID)” on page 75
3 Log in to the Brocade software portal to generate and obtain the license file.	“Obtaining a license” on page 69
4 Upload the license file to the Brocade device.	“Installing a license file” on page 73
5 Verify that the license is installed.	“Verifying the license file installation” on page 74

Obtaining a license

The procedures in this section show how to generate and obtain a software license.

1. Order a license for the desired licensed feature. Refer to [Table 9](#) for a list of valid part numbers and licensed features.

NOTE

To order and obtain a *trial license*, contact your Brocade representative.

2. You can obtain the LID two ways:

- You can also obtain the LID from the IUID label on the unit.
- You receive the paper-pack or electronic transaction key, retrieve the LID of your Brocade device by entering the **show version** command on the device. Example command output is shown in [“Viewing the License ID \(LID\)”](#) on page 75.”

If you received a paper-pack transaction key, write the LID in the space provided on the entitlement certificate.

NOTE

Do not discard the entitlement certificate or e-mail with electronic key. Keep it in a safe place in case it is needed for technical support or product replacement (RMAs).

3. Log in to the Brocade software portal at <http://swportal.brocade.com> and complete the software license request. If you do not have a login ID and password, request access by following the instructions on the screen.

Figure 1 shows the **Software Portal Login** window.

FIGURE 1 Brocade Software Portal Login window

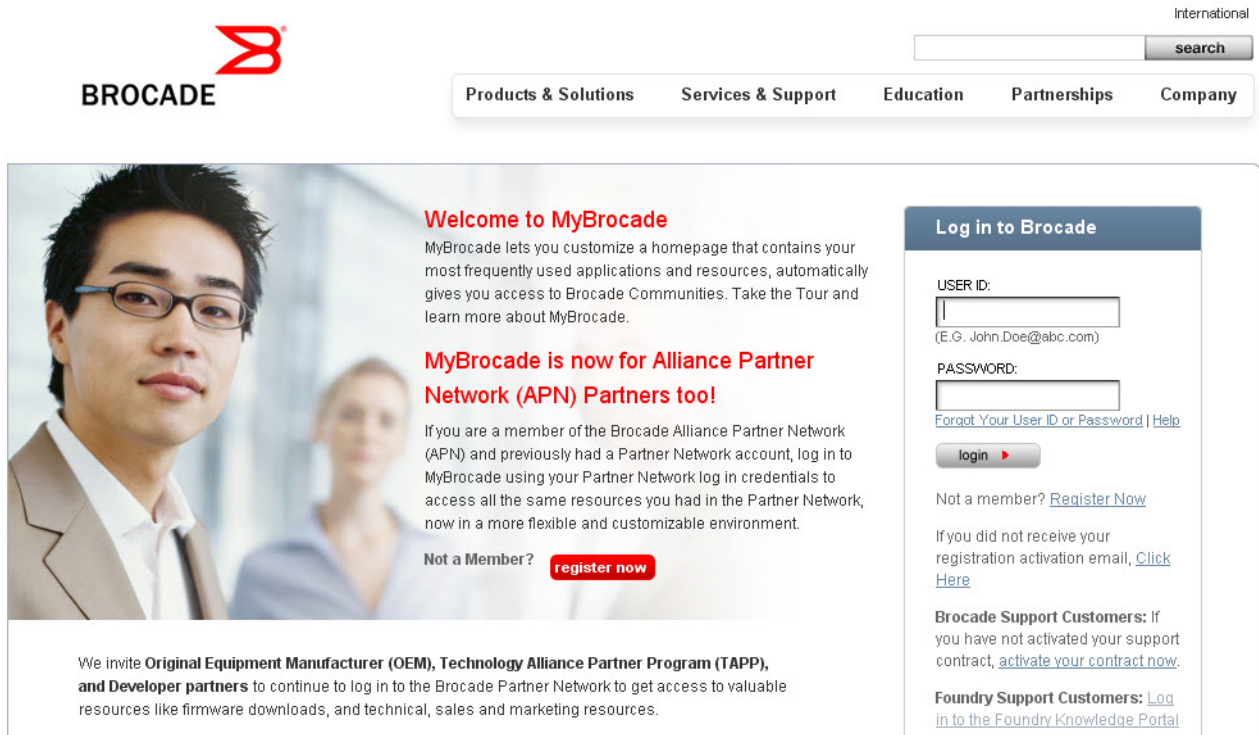


Figure 2 shows the **License Management Welcome** window that appears after logging in to the software portal. From this window, mouse over the **License Management** banner, then **Brocade IP/Ethernet**, then click on **License Generation with Transaction key**.

FIGURE 2 License Management Welcome window

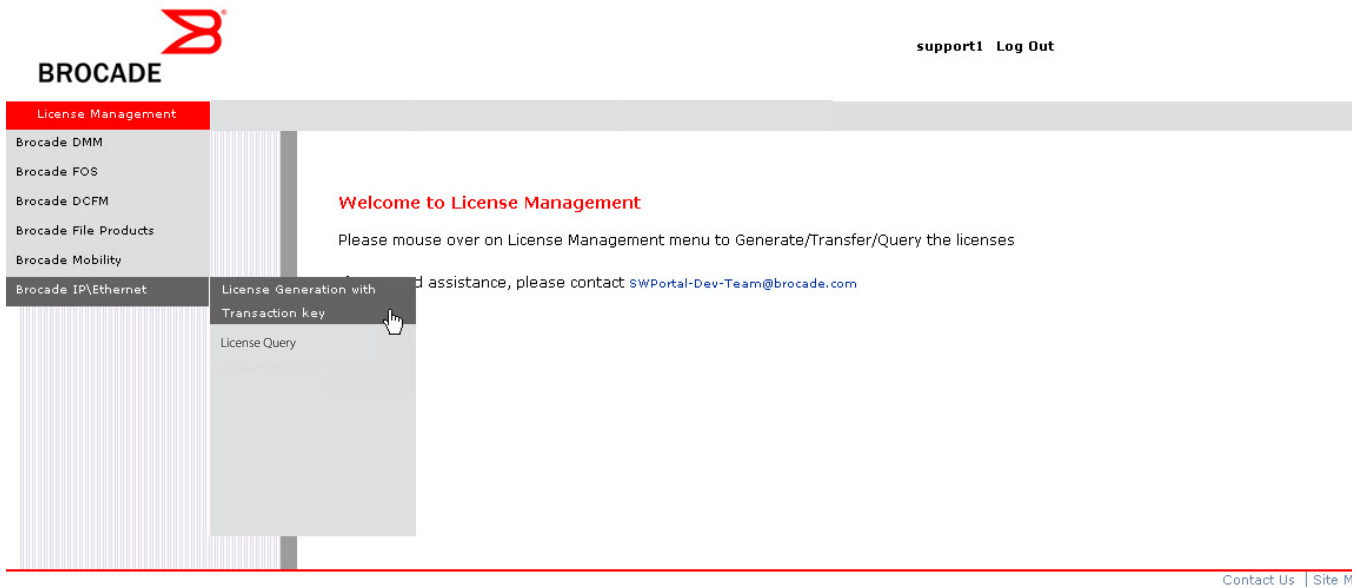


Figure 3 shows the **IP/Ethernet License Generation** window for generating a license using a transaction key and LID.

FIGURE 3 IP Ethernet License Generation window

The screenshot shows the Brocade License Management web interface. At the top left is the Brocade logo and the text "BROCADE". To the right, there are links for "support1" and "Log Out". Below the logo is a "License Management" header. The main content area is titled "IP/Ethernet License Generation" and includes a red warning: "Please check the Unique ID to make sure it is correct! License install failure may result!".

The form is divided into three sections:

- Customer Information:** A form with fields for Customer email ID* (required), Site Name, Technical Contact, Company Name, City, State/Province, Zip/Postal Code, Country (a dropdown menu currently showing "Select Country"), and Phone.
- E-mail Notification Information:** A form with a "Self" field containing "support1@brocade.com" and an "Other e-mail address(es)" field with a checkbox.
- Unit Information:** A form with fields for Unique ID Type* (dropdown menu showing "LID"), Unit's Unique ID* (required), and Transaction Key* (required). Below these fields is an "Add" button.

At the bottom of the form, there is a checkbox labeled "I have read and accept the Brocade End User License Agreement" and two buttons: "Generate" and "Cancel".

[Contact Us](#)

Enter the required information in each text box shown in Figure 3.

- For a description of the field, move the mouse pointer over the text box.
- An asterisk next to a field indicates that the information is required.
- You can generate more than one license at a time. For each license request, enter the Unit Information (Unit ID and transaction key) then click on the **Add** button.

When you have finished entering the required information, read the Brocade End User License Agreement, then click on the check box to indicate that you have read and accept it.

Press the **Generate** button to generate the license. Figure 4 shows the results window, which displays an order summary and the results of the license request.

- If the license request was successful, the “Status” field will indicate **Success** and the “License File” field will contain a hyperlink to the generated license file. The license file will also be automatically emailed to the specified Customer email ID.
- If the license request failed, the “Status” field will indicate the reason it failed and the action to be taken.

FIGURE 4 IP/Ethernet License Generation Results window

IP/Ethernet License Generation- Result

Customer Information

Customer email ID partner501@company.com
 Site Name
 Technical Contact
 Company Name
 City
 State/Province
 Zip/Postal Code
 Country
 Phone

Following Generated Licenses have been sent to Email ID(s): **partner501@company.com**

ID Type	Unique Id	Transaction Key	Description	Status	License File
LID	pkeguceGFHM	A0D57D0038E39D9427131B	BR-NI-CES-2048-L3U	Success	License Key

[Generate Another License](#)

4. Download the license file to your PC by either clicking on the hyperlink or saving it from the e-mail attachment.
5. Upload the license file to the Brocade device as instructed in the section “[Installing a license file](#)” on page 73.

Installing a license file

Once you obtain a license file, place it on a TFTP or SCP server to which the Brocade device has access, then use TFTP or SCP to copy the file to the license database of the Brocade device.

Using TFTP to install a license file

To copy a license file from a TFTP server to the license database of the Brocade device, enter a command such as the following at the Privileged EXEC level of the CLI:

```
NetIron# copy tftp license 10.1.1.1 lic.xml
```

Syntax: `copy tftp license <IP_address> <license_filename_on_host>`

<IP_address> is the address of the IPv4 TFTP server.

<license_filename_on_host> is the filename of the license file.

Using Secure Copy (SCP) to install a license

SSH and SCP must be enabled on the Brocade device before the procedures in this section can be performed. For details, see the chapter [“Configuring SSH2 and SCP”](#) on page 1423.

To copy a license file from an SCP-enabled client to the license database of the Brocade device, enter a command such as the following on the SCP-enabled client.

```
c:\scp c:\license\license101 terry@10.1.1.1:license
```

Syntax: `scp <license_file_on_host> <user>@<IP_address>:license`

Verifying the license file installation

Use the **show license** command to verify that the license is installed on the device. Details about this command are in the section [“Viewing the license database”](#) on page 76.

Using a trial license

NOTE

A trial license must be ordered and installed by Brocade representative.

A trial license enables demonstration and evaluation of a licensed feature and can be valid for a period of up to 45 days. A licensed feature operating under a trial license has the same functionality (CLI and **show** commands) as does a licensed feature operating under a normal license.

What happens when a trial license expires

A trial license expires when it exceeds the specified expiration time or date. The countdown starts when the trial license is generated. When the license expires, the CLI commands related to the licensed feature will no longer be available from the CLI. The licensed feature will continue to run as configured until the system is reloaded, at which time the feature will be disabled and removed.

NOTE

Trial licenses are not cumulative. The new license replaces the current license. To extend the license, you must contact your Brocade representative.

Console, Syslog, and trap messages for trial license expiration

Three days prior to the date that a trial license is set to expire, the following warning message will appear daily on the console. Syslog and trap messages will also be generated.

```
SYSLLOG: <12>Jan 1 00:00:00 624-top License: Package NI-CES-2024-L3U with LID  
egut-cd0J expires in 3 days
```

On the day that the license will expire, a warning message will appear every two hours.

```
SYSLOG: <12>Jan 1 00:00:00 624-top License: Package NI-CES-2024-L3U with LID egut-cdOJ expires in 4 hours
```

When the license has expired, the following message will appear on the console. Syslog and trap messages will also be generated.

```
SYSLOG: <13>Jan 1 00:00:00 624-top License: NI-CES-2024-L3U with LID egut-cdOJ has expired
```

Renewing or extending a trial license

A trial license can be extended once by another trial license of the same type, or by a normal license of the same type. To avoid any interruptions to the network, obtain and install the second trial license before the first license expires. When extended by another trial license, the duration is not cumulative. The countdown starts when the trial license is generated.

To extend the license, you must contact your Brocade representative.

NOTE

The start and end date of each trial license is pre-defined, based on the date and time it is generated.

Viewing information about software licenses

This section describes the **show** commands associated with software licensing. These commands are issued on the Brocade device, at any level of the CLI.

NOTE

You can also view information about software licenses from the Brocade software portal. Refer to [“Viewing software license information”](#) on page 78.

Viewing the License ID (LID)

Brocade devices that ship during and after the release of software licensing will have the LID imprinted on the label affixed to the device. You also can use the CLI command **show version** to view the LID on these devices, and on devices that shipped before the release of software licensing.

Use the **show version** command to display the serial number, license, and LID of the device. The following is example output from an CES unit with the license L3_PREM installed.

```
NetIron#show version
System: NetIron CES (Serial #: SA18091219, Part #: 36003-002C)
License: L3_PREM (LID: ucGNFOGHGO)
Boot      : Version 5.0.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr  3 2010 at 18:43:56 labeled as ceb05000
(443103 bytes) from boot flash
Monitor   : Version 5.0.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr  3 2010 at 18:43:56 labeled as ceb05000
(443103 bytes) from code flash
IronWare  : Version 5.0.0T183 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr  3 2010 at 19:46:12 labeled as ce05000
(11610682 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000c
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
512 MB DRAM
System uptime is 3 days 4 hours 31 minutes 57 seconds
```

Viewing the license database

To display general information about all software licenses in the license database, use the **show license** command. The following shows example output.

```
NetIron# show license
Index      Package Name      Lid      License Type      Status      License Period
1          NI-CES-2048-L3U  ucGNFOGHGO  normal            active      unlimited
```

To display detailed information about a particular license, use the **show license <index_number>** command. The following shows example output.

```
NetIron# show license 1
License information for license <1>:
+package name:      NI-CES-2048-L3U
+lid:               ucGNFOGHGO
+license type:      normal
+status:            active
+license period:    unlimited
```

Syntax: **show license** [<index_number>]

The following table describes the information displayed by the **show license** command.

TABLE 12 Output from the **show license** command

This field...	Displays...
Index	The license hash number that uniquely identifies the license.
Package Name	The package name for the license.
Lid	The license ID. This number is embedded in the Brocade device.
License Type	Indicates whether the license is normal (permanent) or trial (temporary).

TABLE 12 Output from the **show license** command (Continued)

This field...	Displays...
Status	Indicates the status of the license: <ul style="list-style-type: none"> • Valid – A license is valid when the LID matches the serial number of the device for which the license was purchased, and the package name is recognized by the system. • Active – The license is valid and in effect on the device. • Not used – The license is not in effect on the device. • Expired – For trial licenses only, this indicates that the trial license has expired.
License Period	If the license type is trial (temporary), this field will display the number of days the license is valid. If the license type is normal (permanent), this field will display “unlimited”.
Trial license information	
The following details display in the output of the show license <Index_number> command.	
+ days used	The number of days the trial license has been in effect.
+ hours used	The number of hours the trial license has been in effect.
+ days left	The number of days left before the trial license expires.
+ hours left	The number of hours left before the trial license expires.

Viewing active packages installed in the device

Use the **show version** command to view the active packages that are currently installed in the device.

NOTE

The active package name is not the same as the license name.

```

NetIron# show version
System: NetIron CES (Serial #: SA18091219, Part #: 36003-002C)
License: L3_PREM (LID: ucGNFOGHGO)
Boot : Version 5.0.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr 3 2010 at 18:43:56 labeled as ceb05000
(443103 bytes) from boot flash
Monitor : Version 5.0.0T185 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr 3 2010 at 18:43:56 labeled as ceb05000
(443103 bytes) from code flash
IronWare : Version 5.0.0T183 Copyright (c) 1996-2009 Brocade Communications
Systems, Inc.
Compiled on Apr 3 2010 at 19:46:12 labeled as ce05000
(11610682 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000c
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
512 MB DRAM
System uptime is 3 days 4 hours 31 minutes 57 seconds

```

Table 13 lists the supported software packages.

TABLE 13 Software packages

Product	Software package name	License needed?
NetIron CES	NetIron CES 2000 Series BASE	No
	NetIron CES 2000 Series ME_PREM	Yes
	NetIron CES 2000 Series L3_PREM	Yes
NetIron CER	CER 2000 Series BASE	No
	CER 2000 Series ADV_SVCS_PREM	Yes

Deleting a license

A license will remain in the license database until it is deleted. If you want to delete a license, Brocade recommends that you first disable the licensed feature before deleting the associated license.

To delete a license, enter a command such as the following at the Privileged EXEC level of the CLI:

```
NetIron# license delete 1
```

This command immediately removes the license from the license database. The CLI commands related to the licensed feature will no longer be available from the CLI. The licensed feature will continue to run as configured until the software is reloaded, at which time the feature will be disabled and removed from the system. Syslog and trap messages are generated when the license is deleted.

Syntax: `license delete <index_number>`

`<index_number>` is a valid license index number. This information can be retrieved from the `show license` command output. For more information, refer to “” on page 81.

Other licensing options available from the Brocade Software Portal

This section describes other software licensing tasks supported from the Brocade software portal.

Viewing software license information

You can use the **License Query** option to view software license information for a particular unit, transaction key, or both. You can export the report to Excel for sharing or archiving purposes.

Depending on the status of the license, for example whether or not the license was generated, the report will include the following Information:

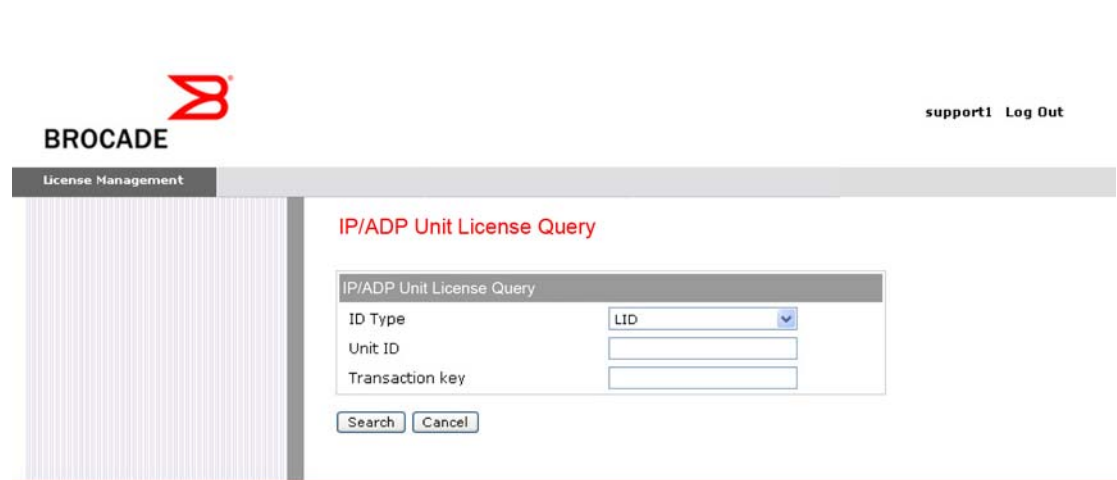
- Hardware part number, serial number, and description
- Software part number, serial number, and description
- Date the license was installed
- Transaction key

- LID
- Feature name
- Product line

To access the License Query option, select it from the **License Management Welcome** window shown in Figure 2.

Figure 5 shows the **License Query** window.

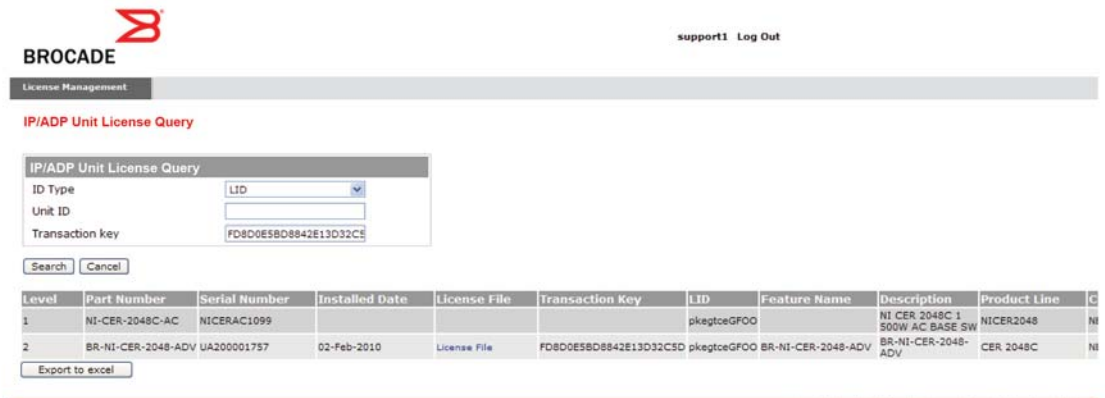
FIGURE 5 License Query window



- To view software license information for a particular unit, enter the LID in the **Unit ID** field then click on **Search**.
- To view software license information for a particular transaction key, enter the unique number in the **Transaction key** field then click on **Search**.

Figure 6 shows an example of the license query results.

FIGURE 6 License Query results window



In this example, the line items for **Level 1** display hardware-related information and the line items for **Level 2** display software-related information. If the query was performed before the transaction key was generated, the first row (**Level 1**) would not appear as part of the search results. Similarly, if the query was performed before the license was generated, some of the information in the second row would not be displayed.

Transferring a license

A license can be transferred between Brocade devices if the following conditions are true:

- The device is under an active support contract, and
- The license is being transferred between two like-models (e.g., from a 24-port model to another 24-port model or from a 48-port model to another 48-port model).

NOTE

A license transfer is intended for retrieving licenses from defective units. The licenses are removed from the defective unit in our database and the unit is flagged as removed from service.

NOTE

Transferring a license is only available internally for TAC, and externally for designated partners with specific accounts in the Software Portal. Contact your Brocade representative for more information.

Special replacement instructions for legacy devices

A **legacy device** refers to a Brocade device that was shipped prior to the introduction of software-based licensing, has an EEPROM installed, and is running pre-release 05.0.00 software.

For Brocade legacy devices in need of replacement (via a Return Merchandise Agreement (RMA)), the following actions must be taken:

- If the replacement device will be upgraded to a software release that supports software-based licensing, registration of the replacement device is required after the software is upgraded. To register the device, follow the instructions in [“Special replacement instructions for legacy devices”](#) on page 80.
- If the replacement device will be using a software release that does *not* support software-based licensing, follow these instructions:
 1. Prior to shipping the device in need of replacement back to the factory, remove the EEPROM from the device. To remove the EEPROM, follow the instructions in the appropriate hardware installation guide or in the instructions that shipped with the EEPROM.
 2. After removing the EEPROM, store it in a safe place.
 3. When the replacement device is received from the factory, install the same EEPROM in the device. To do so, follow the instructions that shipped with the EEPROM.

Syslog messages and trap information

Table 14 lists the syslog messages and traps supported for software-based licensing.

TABLE 14 Syslog messages

Message level	Message	Explanation
Informational	License: Package <package_name> with LID <LID_number> is added	Indicates that the license package has been added.
Informational	License: Package <package_name> with LID <LID_number> is removed	Indicates that the license package has been deleted.
Warning	License: Package <package_name> with LID <LID_number> expires in <number> days	The trial license is about to expire. This message will begin to display 3 days before the expiration date, and every day until the license will expire.
Warning	License: Package <package_name> with LID <LID_number> expires in <number> hours	The trial license is about to expire. This message will begin to display every 2 hours on the last day that the license will expire.
Notification	License: Package <package_name> with LID <LID_number> has expired	The trial license has expired.

8 Syslog messages and trap information

Loading and saving configuration files

This chapter contains information you will need to know when loading and saving configuration files on your Brocade device.

Brocade MLX Series and Brocade NetIron XMR devices

For easy configuration management, the router supports both the download and upload of configuration files between the router and a TFTP server on the network.

You can upload either the startup configuration file or the running configuration to the TFTP server, code flash, or a flash card for backup and use in booting the system.

Startup configuration file – This file (startup-config) contains the configuration information that is currently saved in the flash memory. To display this file, enter the **show configuration** command at any CLI prompt.

Running configuration – This active configuration is in the system RAM but not yet saved to flash memory. These changes could represent a short-term requirement or general configuration change. To display this configuration, enter the **show running-config** or **write terminal** command at any CLI prompt.

Each device can have one startup configuration file and one running configuration. The startup configuration file is shared by both flash modules. The running configuration resides in DRAM.

Configuring file size for startup and running configuration

The system allocates 8 MB of contiguous memory per session (console, TELNET, SSH) for processing different configuration commands, such as **show run**, **config terminal**, and **copy tftp run**. In a low memory state, memory is generally fragmented resulting in a failure to allocate contiguous memory to support the session. We now pre-allocate one configuration buffer so that at least one CLI session will remain operational even in low memory condition.

NOTE

Low memory is not a normal operating condition, and may indicate scaling the network beyond system max limits. However, this feature ensures that one CLI session remains operational so you can recover from the condition.

To specify a configuration file size for both startup and running configuration, enter the following command:

```
Brocade(config)# system-max
```

Syntax: [no] **system-max** [config-file-size <decimal>]

By default, **no system-max parameter** is configured.

The **config-file-size** option specifies the configuration file size for processing various commands.

The *<decimal>* parameter specifies the range supported for configuring file size. The minimum configuration is 2 MB, and the maximum is 16 MB. If the file size is not configured, the default size of 8 MB is used.

NOTE

It is strongly recommended that you use the default size (8 MB) when configuring file size.

When you enter the **system-max** command, with the `config-file-size` parameter included, the following additional information is displayed:

```
Brocade(config)# system-max config-file-size 2097152
Reload required. Please write memory and then reload or power cycle.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
Replacing the Startup Configuration with the Running Configuration
```

NOTE

You must enter the **write memory** command and restart the system for this command to take effect.

Replacing the startup configuration with the running configuration

After you make configuration changes to the active system, you can save the changes to flash memory, which replaces the existing startup configuration with the new running configuration.

To replace the startup configuration with the new running configuration, enter the **write memory** command.

```
Brocade# write memory
```

Retaining the current startup configuration

After making configuration changes to the active system, if you have not executed a **write memory** command and you decide you don't want to save the changes, enter the **reload** command to return to the current startup configuration.

```
Brocade# reload
```

If the system detects differences between the running and startup configurations, it prompts you as follows:

```
Are you sure? (enter 'y' or 'n'):
```

Enter **y**, and press the **Enter** key.

Copying a configuration file to or from an SCP or TFTP server

To copy the startup-config or running-config file to or from an SCP or TFTP server, use the commands shown in this section.

NOTE

You can name the configuration file when you copy it to an SCP or TFTP server. However, when you copy a configuration file from the server to a device, the file is always copied as “startup-config” or “running-config”, depending on which type of file you saved to the server.

Using TFTP

To copy the startup-configuration files to a TFTP server, enter the following command:

```
copy startup-config tftp <ip-address> <filename>
```

To upload the running-config from the device to a TFTP server, enter the following command:

```
copy running-config tftp <ip-address> <filename>
```

To upload a copy of the startup-config to the device from a TFTP server, enter the following command.

```
copy tftp startup-config <ip-address> <filename>
```

To upload a running configuration to the device from a TFTP server, enter the following command:

```
copy tftp running-config <tftp -srvr> <filename> [overwrite]
```

This command downloads the access-list to the running-configuration. The new access-list is then appended to the current running configuration of the router.

Using SCP

Running configuration backup or appending via scp

To copy the running configuration file on a device to a file on the SCP-enabled host.

```
C:\> scp <user>@<device-IpAddress>:runConfig <dst-file>
```

To download a configuration file and append to running configuration, enter the following command.

```
C:> scp <config-file> <user>@<device-IpAddress>:config:run
```

This command transfers <config-file> to the device and appends to the running configuration.

For backward compatibility, the following syntax is also supported for this command.

```
C:> scp <config-file> <user>@<device-IpAddress>:runConfig
```

Replacing or backing up the startup configuration using SCP

To copy the startup configuration file on the device to a file on the SCP-enabled client, enter the following command:

```
C:> scp <user>@<device-IpAddress>:startConfig <dst-file>
```

To download a configuration file and replace the startup configuration, enter the following command.

```
C:> scp <config-file> <user>@<device-IpAddress>:config:start
```

This command transfers *<config-file>* to the device and replaces the startup configuration in flash.

For backward compatibility, the following syntax is also supported for this command.

```
C:> scp <config-file> <user>@<device-IpAddress>:startConfig
```

Making local copies of the startup configuration file

You can copy the startup-config file in flash memory to a TFTP server or to a PCMCIA flash card inserted in management module slot 1 or 2.

For example, to make a backup copy of the startup-config file and save the backup file to a TFTP server, enter a command such as the following at the Privileged EXEC level in the CLI:

```
Brocade# copy startup-config tftp 10.28.40.21 startup-config.bak
```

Syntax: **copy startup-config tftp** *<ip-address>* *<dest-file-name>*

The *<ip-address>* variable specifies the IP address of the TFTP server that you want to save the startup configuration to.

The *<dest-file-name>* specifies the name of the file you copied to a new destination.

For example, to make a backup copy of the startup-config file and save the backup file on a flash card in slot 2, enter a command such as the following at the Privileged EXEC level in the CLI:

```
Brocade# copy startup-config slot2 /backups/startup-config.bak
```

Syntax: **copy startup-config [slot1 | slot2]** [*<dest-dir-path>*]/*<dest-file-name>*

Specify the *<dest-dir-path>* parameter to copy the source file to a file system that does not have current management focus.

The *<dest-file-name>* parameter specifies the name of the file you copied to a new destination.

NetIron CES Series and NetIron CER devices

For easy configuration management, the device supports both the download and upload of configuration files between the router and a TFTP server on the network.

Startup configuration file – This file (startup-config) contains the configuration information that is currently saved in the Brocade NetIron CER and Brocade NetIron CES series flash memory. To display this file, enter the **show configuration** command at any CLI prompt.

Running configuration – This active configuration is in the system RAM but not yet saved to flash memory. These changes could represent a short-term requirement or general configuration change. To display this configuration, enter the **show running-config** or **write terminal** command at any CLI prompt.

Each device can have one startup configuration file and one running configuration. The startup configuration file is shared by both flash modules. The running configuration resides in DRAM.

Configuring file size for startup and running configuration

The system allocates 8 MB of contiguous memory per session (console, TELNET, SSH) for processing different configuration commands, such as **show run**, **config terminal**, and **copy tftp run**. In a low memory state, memory is generally fragmented resulting in a failure to allocate contiguous memory to support the session. We now pre-allocate one configuration buffer so that at least one CLI session will remain operational even in low memory condition.

NOTE

Low memory is not a normal operating condition, and may indicate scaling the network beyond system max limits. However, this feature ensures that one CLI session remains operational so you can recover from the condition.

To specify a configuration file size for both startup and running configuration, enter the following command:

```
Brocade(config)# system-max
```

Syntax: [no] **system-max** [**config-file-size** <decimal>]

By default, **no system-max parameter** is configured.

The **config-file-size** option specifies the configuration file size for processing various commands.

The <decimal> parameter specifies the range supported for configuring file size. The minimum configuration is 2 MB, and the maximum is 16 MB. If the file size is not configured, the default size of 8 MB is used.

NOTE

Brocade strongly recommended that you use the default size (8 MB) when configuring file size.

When you enter the **system-max** command, with the `config-file-size` parameter included, the following additional information is displayed:

```
Brocade(config)# system-max config-file-size 2097152
Reload required. Please write memory and then reload or power cycle.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
Replacing the Startup Configuration with the Running Configuration
```

NOTE

You must enter the **write memory** command and restart the system for this command to take effect.

Replacing the startup configuration with the running configuration

After you make configuration changes to the active system, you can save the changes to flash memory, which replaces the existing startup configuration with the new running configuration.

To replace the startup configuration with the new running configuration, enter the **write memory** command.

```
Brocade# write memory
```

Retaining the current startup configuration

After making configuration changes to the active system, if you have not executed a **write memory** command and you decide you don't want to save the changes, enter the **reload** command to return to the current startup configuration.

```
Brocade# reload
```

If the system detects differences between the running and startup configurations, it prompts you as follows:

```
Are you sure? (enter 'y' or 'n'):
```

Enter **y**, and press the **Enter** key.

Copying a configuration file to or from an SCP or TFTP server

To copy the `startup-config` or `running-config` file to or from an SCP or TFTP server, use the commands shown in this section.

NOTE

You can name the configuration file when you copy it to an SCP or TFTP server. However, when you copy a configuration file from the server to a device, the file is always copied as “`startup-config`” or “`running-config`”, depending on which type of file you saved to the server.

Using TFTP

To copy startup-configuration files to or from a TFTP server, enter the following command:

```
copy startup-config tftp <ip-address> <filename>
```

To upload the running-config from the device to a TFTP server, enter the following command:

```
copy running-config tftp <ip-address> <filename>
```

To copy a startup-config to the device from a TFTP server, enter the following command.

```
copy tftp startup-config <ip-address> <filename>
```

To upload a running configuration to the device from a TFTP server, enter the following command:

```
copy tftp running-config <tftp -srvr> <filename> [overwrite]
```

This command downloads the access-list to the running-configuration. The new access-list is then appended to the current running configuration of the router.

Using SCP

Running configuration backup or appending via scp

To copy the running configuration file on a device to a file on the SCP-enabled host.

```
C:\> scp <user>@<device-IpAddress>:runConfig <dst-file>
```

To download a configuration file and append to running configuration, enter the following command.

```
C:> scp <config-file> <user>@<device-IpAddress>:config:run
```

This command transfers <config-file> to the device and appends to the running configuration.

For backward compatibility, the following syntax is also supported for this command.

```
C:> scp <config-file> <user>@<device-IpAddress>:runConfig
```

Replacing or backing up the startup configuration using SCP

To copy the startup configuration file on the device to a file on the SCP-enabled client, enter the following command:

```
C:> scp <user>@<device-IpAddress>:startConfig <dst-file>
```

To download a configuration file and replace the startup configuration, enter the following command.

```
C:> scp <config-file> <user>@<device-IpAddress>:config:start
```

This command transfers <config-file> to the device and replaces the startup configuration in flash.

For backward compatibility, the following syntax is also supported for this command.

```
C:> scp <config-file> <user>@<device-IpAddress>:startConfig
```

Making local copies of the startup configuration file

Copy the startup-config file in flash memory to a TFTP server.

For example, to make a backup copy of the startup-config file and save the backup file to a TFTP server, enter a command such as the following at the Privileged EXEC level in the CLI:

```
Brocade# copy startup-config tftp 10.28.40.21 startup-config.bak
```

Syntax: `copy startup-config tftp <ip-address> <dest-file-name>`

The `<ip-address>` variable specifies the IP address of the TFTP server that you want to save the startup configuration to.

The `<dest-file-name>` specifies the name of the file you copied to a new destination.

Device module considerations

This appendix contains information about specific device components that you may find useful when you perform your Multi-Service IronWare software upgrade.

Interface module considerations

The following sections contain upgrade and downgrade information for interface modules. When installing or upgrading interface modules, consider the following:

- 1Gx24 copper and fiber interface modules require software version 5.1.00 or later.
- For interface modules with 24 or more ports, you must change the ifindex. Refer to “[ifIndex allocation](#)” on page 4.
- Before you install your 100GbE interface module into an existing working device, you must change the switch fabric data-mode to force-normal, and the system tm credit size to 1024b (which readies the device to forward 100 Gbps traffic. Change these settings by entering the following commands, writing to memory, and reloading the device.

```
Brocade(config)# system-init fabric-data-mode force-normal
Brocade(config)# system-init tm-credit-size credit_1024b
Brocade(config)# exit
Brocade# write memory
Brocade# reload
```

For more information about how to install 100GbE modules, refer to the *Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide*.

Upgrading high-speed switch fabric modules

The following interface modules require high-speed switch fabric modules to operate:

- NI-MLX-10Gx8-M (requires R05.0.00c or later)
- NI-MLX-10Gx8-D (requires R05.0.00c or later)
- BR-MLX-10Gx8-X (requires R05.2.00 or later)
- BR-MLX-100GX1-X and BR-MLX-100GX2-X (requires R05.2.00 or later)

NOTE

Do not attempt to downgrade the modules or high-speed switch fabric modules listed above to software versions older than R05.0.00c. The modules will not operate with older software.

If you are installing these modules in your device, you must also install high-speed switch fabric modules (if not already installed). For hardware installation instructions, refer to the *Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide*.

When you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D, you must first upgrade the entire system to software R05.0.00c or later, and replace existing switch fabric modules with high-speed switch fabric modules. Be sure to remove all standard switch fabric modules BEFORE you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules.

A Interface module considerations

When you install BR-MLX-10Gx8-X interface modules, you must first upgrade the entire system to software R05.2.00 or later, and replace existing switch fabric modules with high-speed switch fabric modules. Be sure to remove all standard switch fabric modules BEFORE you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules.

NOTE

Do not attempt to downgrade BR-MLX-10Gx8-X modules or high-speed switch fabric modules to software versions older than R05.2.00. The modules will not operate with older software.

If you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D or BR-MLX-10Gx8-X interface modules without high-speed switch fabric modules, the interface modules will not work. For Brocade MLX and Brocade NetIron XMR 16-slot devices, you must also install high-speed fans. Refer to the *Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide* for installation instructions.

To upgrade software and install high-speed switch fabric modules and NI-MLX-10Gx8-M or NI-MLX-10Gx8-D or BR-MLX-10Gx8-X modules at the same time, first upgrade your router to the appropriate software version for your interface modules, then perform the following steps:

NOTE

Traffic may be briefly interrupted during an inline upgrade procedure.

-
1. Upgrade all application, boot, and monitor files, and all management, interface, and switch fabric module FPGAs to R05.0.00c or later (for NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules). For BR-MLX-10Gx8-X interface modules, you must upgrade to R05.2.00 or later.
 2. Restart your device.
 3. Enter the **show version** command to confirm that the upgrade was successful.
 4. Remove a standard switch fabric module.
 5. Install a high-speed switch fabric module in the empty switch fabric slot.
 6. To confirm that the new module is operating properly, enter the **show module** command.
Repeat steps 4 through 6 to replace the remaining switch fabric modules with high-speed switch fabric modules.
 7. Install an interface module into an empty interface module slot.
 8. To confirm that the module is operating properly, enter the **show module** command.
Repeat steps 7 and 8 to install all remaining interface modules.

Troubleshooting

This appendix contains information about specific scenarios and troubleshooting issues that you may find useful when you perform your Multi-Service IronWare software upgrade.

Upgrading devices in MCT topologies

MCT (multi-chassis trunking) does not support hitless upgrades of devices within the MCT topology. However, it is possible to avoid interruptions of traffic flow when upgrading MCT devices. To do this, you must first issue the **client-shutdown** on the device that is being upgraded. This forces all traffic to the other MCT devices. Once the traffic is redirected, perform the upgrade using the standard upgrade procedure, and reload the MCT device while it is still in shutdown mode. When the upgrade is complete, remove the client-shutdown by entering the **no client-shutdown** command and resume forwarding traffic. The commands for this process are shown here.

```
Brocade(config)# cluster abc 1
Brocade(config-cluster-abc)# client-interfaces shutdown
```

Perform the upgrade on this device at this point. When the upgrade is complete, enter the following command to resume traffic flow.

```
Brocade(config-cluster-abc)# no client-interfaces shutdown
```

NOTE

This process must be done separately for each device in the MCT topology. If you attempt an upgrade or reload without issuing the client-shutdown, traffic may be adversely affected for all devices.

Recovering from a failed upgrade

This section describes two scenarios in which you may have to recover from a failed upgrade.

- Upgrade fails, no primary image exists. At reboot, system automatically stops in monitor mode.
- An incorrect version of the software has been loaded on the device. At reboot, the system automatically stops in monitor mode

For either instance, the recovery procedure is the same, and is explained here.

If your upgrade fails, when you issue the reload command, you will see output similar to this example.

```
BOOT INFO: load image from primary copy Bad image header
BOOT INFO: load image from secondary copy File not found, 'secondary'
MP-1Monitor>
```

B Recovering from a failed upgrade

If you issue a **dir** command, you will see information similar to the following.

```
MP-1 Monitor> dir
 524288 [0000] lp-monitor-0
 6505897 [0000] lp-primary-0
 523622 [0000] monitor
 13667494 [0000] primary
 1688 [ac60] startup-config
 21232924 bytes 15 File(s)
7602176 bytes free
MP-1 Monitor>
```

You can recover by copying a new image from a TFTP server, as shown in the following steps.

NOTE

For R05.2.00, recovery can only be achieved by using a TFTP server.

1. Assign an IP address to in monitor mode.

```
MP-1 Monitor> ip address 10.10.10.1/24
IP address = 10.10.10.1
MP-1 Monitor> ip default-gateway 10.10.10.254
```

2. Copy the application image from the TFTP server using the following command:

```
MP-1 Monitor> copy tftp flash 10.10.10.2 xmr05200.bin primary
```

3. Reload the device using the following command. After the reload, the device should be running R05.2.00 (there will be no secondary image).

```
MP-1 Monitor> reset
Are you sure? (enter 'y' or 'n'): y
NetIron XMR/MLX Boot Code Version 5.2.00
..MP.
Enter 'a' to stop at memory test
Enter 'b' to stop at boot monitor
..BOOT INFO: load monitor from code flash, cksum = 79ca monitor 0x80000100
DMAC0 Link is up
BOOT INFO: verify flash files - max_code_flash_blocks[126].....
read_startup_config
INFO: 4-slot backplane is detected.
g_bp_board_class_val = 134, g_max_slave_slot = 4, g_max_snm_slot = 3,
g_max_power = 3
```

Troubleshooting a failed FIPS software image installation

When FIPS is enabled and a signature file does not pass the validation check (does not match the binary file) or is corrupt, the device does not allow the code to finish loading. In this case, cascade reloads occur.

You can interrupt a reload to recover and install another image in monitor mode by completing the following steps:

1. Enter **b** to interrupt the reload. The device enters monitor mode.
2. Assign a remote ip address, subnet mask and default gateway.
ip address <IpAddress>/<CIDR mask>
ip default-gateway <gatewayIp>
3. Using TFTP, you can copy the missing signature file, or downgrade to an earlier version, or boot remotely to a non-FIPS image, such as R05.1.00b, using one of the following commands:
 - To copy the missing signature file:
copy tftp flash <tftp-srvr> <signature-file> <destination-signature-filename>
 - To downgrade to a non-FIPS application (for example, **xmr05100b.bin**)
copy tftp flash <tftp-srvr> **xmr05100b.bin primary**
 - To boot remotely from a TFTP server to a non-FIPS image (for example **xmr05100b.bin**):
boot system tftp <tftp-srvr> **xmr05100b.bin**

B Troubleshooting a failed FIPS software image installation

Patch Upgrade Information for all Supported Devices

For patch releases, in most cases, you do not need to upgrade all images. This appendix lists all images for specific patches.

Required images for R05.2.00c

The following table lists the images that have changed for patch release R05.2.00c. You must upgrade these images for a successful upgrade.

Brocade MLX Series and Brocade NetIron XMR devices

TABLE 15 Required images for a basic R05.2.00c software upgrade

Image description	Image name
Combined application image for management modules	xm05200c.bin
Monitor image for management modules	xmb05200.bin
Monitor image for interface modules	xmlb05200.bin
Boot image for management modules	xmprm05200.bin
Boot image for interface modules	xmlprm05200.bin
Combined FPGA image for interface modules	lpfpga05200c.bin

C Required images for R05.2.00c

TABLE 16 Multi-Service IronWare R05.2.00c image files

Hardware	Image type	Image name	Compatible version	
Management modules	Boot	xmprm05200.bin	n/a	
	Monitor	xmb05200.bin	n/a	
	Application	xmr05200c.bin	n/a	
	Combined application	xm05200c.bin	n/a	
	MBRIDGE	mbridge_05200c.xsvf	36	
	MBRIDGE32	mbridge32_05200c.xsvf (32-slot routers only)	35	
Interface modules	Boot	xmplrm05200.bin	n/a	
	Monitor	xmlb05200.bin	n/a	
	Application	xmlp05200c.bin	n/a	
	Combined FPGA	lpfpga05200c.bin	n/a	
	Individual FPGA images		pbifsp2_05200c.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	3.24
			xppsp2_05200c.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	6.23
			xppoc_05200c.bin (POS interface modules)	7.00
			pbifoc_05200c.bin (POS interface modules)	3.07
			statsoc_05200c.bin (POS interface modules)	2.06
			pbifmrj_05200c.bin (24x1G and 48x1G modules)	3.26
			xppmrj_05200c.bin (24x1G and 48x1G modules)	7.01
			statsmrj_05200c.bin (24x1G and 48x1G modules)	0.09
			pbif8x10_05200c.bin (8x10G modules)	1.18
			xpp8x10_05200c.bin (8x10G modules)	3.26
	xgmacsp2_05200c.bin (2x10G and 4x10G modules)	0.15		
	xpp2x100_05200c.bin (2x100G modules)	3.02		
Switch fabric modules	SBRIDGE	sbridge_05200c.mcs	6	
High speed switch fabric modules	HSBRIDGE	hsbridge_05200c.mcs	16	

Brocade NetIron CES and Brocade NetIron CER devices

TABLE 17 Required images for a basic R05.2.00c software upgrade

Image description	Image name
Application - Multi-Service IronWare	ce05200c.bin
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin
fpga-pbif image	pbifmetro_05200c.bin

FIPS R05.2.00c images

FIPS enabled Brocade MLX Series and Netron XMR devices

TABLE 18 Required images for a FIPS enabled basic upgrade to R05.2.00c

Required image	Image name	Signature file name
Combined application image for management modules	xm05200c.bin	xmr05200b.sig xmpl05200b.sig
Monitor image for management modules	xmb05200.bin	xmb05200.sig
Monitor image for interface modules	xmlb05200.bin	xmlb05200.sig
Boot image for management modules	xmprm05200.bin	xmprm05200.sig
Boot image for interface modules	xmlprm05200.bin	xmlprm05200.sig
Combined FPGA image for interface modules	lpfpga05200c.bin	lpfpga05200c.sig

TABLE 19 FIPS enabled Multi-Service IronWare R05.2.00c image files

Hardware	Image type	Image name	Signature file name	Compatible version	
Management modules	Boot	xmprm05200.bin	xmprm05200.sig	n/a	
	Monitor	xmb05200.bin	xmb05200.sig	n/a	
	Application	xmr05200c.bin	xmr05200c.sig	n/a	
	Combined application	xm05200c.bin	xm05200c.sig	n/a	
	MBRIDGE	mbridge_05200c.xsvf	mbridge_05200c.sig	36	
	MBRIDGE32	mbridge32_05200c.xsvf (32-slot routers only)	mbridge32_05200c.sig	35	
Interface modules	Boot	xmlprm05200.bin	xmlprm05200.sig	n/a	
	Monitor	xmlb05200.bin	xmlb05200.sig	n/a	
	Application	xmpl05200c.bin	xmpl05200c.sig	n/a	
	Combined FPGA	lpfpga05200c.bin	lpfpga05200c.sig	n/a	
	Individual FPGA images		pbifsp2_05200c.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	pbifsp2_05200c.sig	3.24
			xppsp2_05200c.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	xppsp2_05200c.sig	6.23
			xppoc_05200c.bin (POS interface modules)	xppoc_05200c.sig	6.22
			pbifoc_05200c.bin (POS interface modules)	pbifoc_05200c.sig	3.06
			statsoc_05200c.bin (POS interface modules)	statsoc_05200c.sig	2.06
			pbifmrj_05200c.bin (24x1G and 48x1G modules)	pbifmrj_05200c.sig	3.25
			xppmrj_05200c.bin (24x1G and 48x1G modules)	xppmrj_05200c.sig	6.24
			statsmrj_05200c.bin (24x1G and 48x1G modules)	statsmrj_05200c.sig	0.09
			pbif8x10_05200c.bin (8x10G modules)		
			xpp8x10_05200c.bin (8x10G modules)	pbif8x10_05200c.sig	1.14
			xgmacsp2_05200c.bin (2x10G and 4x10G modules)	xpp8x10_05200c.sig	3.08
				xgmacsp2_05200c.sig	0.15
			xpp2x100_05200c.bin (2x100G modules)		
		xpp2x100_05200c.sig	2.22		
Switch fabric modules	SBRIDGE	sbridge_05200c.mcs	sbridge_05200c.sig	6	
High speed switch fabric modules	HSBRIDGE	hsbridge_05200c.mcs	hsbridge_05200c.sig	16	

C Required images for R05.2.00c

FIPS enabled Brocade NetIron CES and Brocade NetIron CER devices

TABLE 20 Required images for a FIPS enabled upgrade to R05.2.00c

Required image	Binary image name	Signature Image name	Signature Filename on Flash
Application - Multi-Service IronWare	ce05200c.bin	ce05200c.sig	primary.sig
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin	ceb05100.sig	monitor.sig, boot.sig
fpga-pbif image	pbifmetro_05200c.bin	pbifmetro_05200c.sig	pbifmetro.sig

Required images for R05.2.00b

The following table lists the images that have changed for patch release R05.2.00b. You must upgrade these images for a successful upgrade.

Brocade MLX Series and Brocade NetIron XMR devices

TABLE 21 Required images for a basic R05.2.00b software upgrade

Image description	Image name
Combined application image for management modules	xm05200b.bin
Monitor image for management modules	xmb05200.bin
Monitor image for interface modules	xmlb05200.bin
Boot image for management modules	xmprm05200.bin
Boot image for interface modules	xmlprm05200.bin
Combined FPGA image for interface modules	lpfpga05200b.bin

TABLE 22 Multi-Service IronWare R05.2.00b image files

Hardware	Image type	Image name	Compatible version	
Management modules	Boot	xmprm05200.bin	n/a	
	Monitor	xmb05200.bin	n/a	
	Application	xmr05200b.bin	n/a	
	Combined application	xm05200b.bin	n/a	
	MBRIDGE	mbridge_05200b.xsvf	36	
	MBRIDGE32	mbridge32_05200b.xsvf (32-slot routers only)	35	
Interface modules	Boot	xmlprm05200.bin	n/a	
	Monitor	xmlb05200.bin	n/a	
	Application	xmlp05200b.bin	n/a	
	Combined FPGA	lpfpga05200b.bin	n/a	
	Individual FPGA images		pbifsp2_05200b.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	3.24
			xppsp2_05200b.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	6.23
			xppoc_05200b.bin (POS interface modules)	6.22
			pbifoc_05200b.bin (POS interface modules)	3.06
			statsoc_05200b.bin (POS interface modules)	2.06
			pbifmrj_05200b.bin (24x1G and 48x1G modules)	3.25
			xppmrj_05200b.bin (24x1G and 48x1G modules)	6.24
			statsmrj_05200b.bin (24x1G and 48x1G modules)	0.09
			pbif8x10_05200b.bin (8x10G modules)	1.14
			xpp8x10_05200b.bin (8x10G modules)	3.08
		xgmacsp2_05200b.bin (2x10G and 4x10G modules)	0.15	
		xpp2x100_05200b.bin (2x100G modules)	2.22	
	Switch fabric modules	SBRIDGE	sbridge_05200b.mcs	6
High speed switch fabric modules	HSBRIDGE	hsbridge_05200b.mcs	16	

Brocade NetIron CES and Brocade NetIron CER devices

TABLE 23 Required images for a basic R05.2.00b software upgrade

Image description	Image name
Application - Multi-Service IronWare	ce05200b.bin
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin
fpga-pbif image	pbifmetro_05200b.bin

FIPS R05.2.00b images

FIPS enabled Brocade MLX Series and NetIron XMR devices

TABLE 24 Required images for a FIPS enabled basic upgrade to R05.2.00b

Required image	Image name	Signature file name
Combined application image for management modules	xm05200b.bin	xmr05200b.sig xmlp05200b.sig
Monitor image for management modules	xmb05200.bin	xmb05200.sig
Monitor image for interface modules	xmlb05200.bin	xmlb05200.sig
Boot image for management modules	xmprm05200.bin	xmprm05200.sig
Boot image for interface modules	xmlprm05200.bin	xmlprm05200.sig
Combined FPGA image for interface modules	lfpfga05200b.bin	lfpfga05200b.sig

TABLE 25 FIPS enabled Multi-Service IronWare R05.2.00b image files

Hardware	Image type	Image name	Signature file name	Compatible version			
Management modules	Boot	xmprm05200.bin	xmprm05200.sig	n/a			
	Monitor	xmb05200.bin	xmb05200.sig	n/a			
	Application	xmr05200b.bin	xmr05200b.sig	n/a			
	Combined application	xm05200b.bin	xm05200b.sig	n/a			
	MBRIDGE	mbridge_05200b.xsvf	mbridge_05200b.sig	36			
	MBRIDGE32	mbridge32_05200b.xsvf (32-slot routers only)	mbridge32_05200b.sig	35			
Interface modules	Boot	xmplrm05200.bin	xmplrm05200.sig	n/a			
	Monitor	xmlb05200.bin	xmlb05200.sig	n/a			
	Application	xmlp05200b.bin	xmlp05200b.sig	n/a			
	Combined FPGA	lpfpga05200b.bin	lpfpga05200b.sig	n/a			
	Individual FPGA images		pbifsp2_05200b.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	pbifsp2_05200b.sig	3.24		
			xppsp2_05200b.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	xppsp2_05200b.sig	6.23		
			xppoc_05200b.bin (POS interface modules)	xppoc_05200b.sig	6.22		
			pbifoc_05200b.bin (POS interface modules)	pbifoc_05200b.sig	3.06		
			statsoc_05200b.bin (POS interface modules)	statsoc_05200b.sig	2.06		
			pbifmrj_05200b.bin (24x1G and 48x1G modules)	pbifmrj_05200b.sig	3.25		
			xppmrj_05200b.bin (24x1G and 48x1G modules)	xppmrj_05200b.sig	6.24		
			statsmrj_05200b.bin (24x1G and 48x1G modules)	statsmrj_05200b.sig	0.09		
			pbif8x10_05200b.bin (8x10G modules)	pbif8x10_05200b.sig	1.14		
			xpp8x10_05200b.bin (8x10G modules)	xpp8x10_05200b.sig	3.08		
			xgmacsp2_05200b.bin (2x10G and 4x10G modules)	xgmacsp2_05200b.sig	0.15		
			xpp2x100_05200b.bin (2x100G modules)	xpp2x100_05200b.sig	2.22		
			Switch fabric modules	SBRIDGE	sbridge_05200b.mcs	sbridge_05200b.sig	6
			High speed switch fabric modules	HSBRIDGE	hsbridge_05200b.mcs	hsbridge_05200b.sig	16

FIPS enabled Brocade NetIron CES and Brocade NetIron CER devices

TABLE 26 Required images for a FIPS enabled upgrade to R05.2.00b

Required image	Binary image name	Signature Image name	Signature Filename on Flash
Application - Multi-Service IronWare	ce05200b.bin	ce05200b.sig	primary.sig
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin	ceb05100.sig	monitor.sig, boot.sig
fpga-pbif image	pbifmetro_05200b.bin	pbifmetro_05200b.sig	pbifmetro.sig

Required images for R05.2.00a

The following table lists the images that have changed for patch release R05.2.00a. You must upgrade these images for a successful upgrade.

Brocade MLX Series and NetIron XMR devices

TABLE 27 Required images for a basic R05.2.00a software upgrade

Image description	Image name
Combined application image for management modules	xm05200a.bin
Monitor image for management modules	xmb05200.bin
Monitor image for interface modules	xmlb05200.bin
Boot image for management modules	xmprm05200.bin
Boot image for interface modules	xmlprm05200.bin
Combined FPGA image for interface modules	lpfpga05200a.bin

TABLE 28 Multi-Service IronWare R05.2.00a image files

Hardware	Image type	Image name	Compatible version	
Management modules	Boot	xmprm05200.bin	n/a	
	Monitor	xmb05200.bin	n/a	
	Application	xmr05200a.bin	n/a	
	Combined application	xm05200a.bin	n/a	
	MBRIDGE	mbridge_05200a.xsvf	32	
	MBRIDGE32	mbridge32_05200a.xsvf (32-slot routers only)	33	
Interface modules	Boot	xmlprm05200.bin	n/a	
	Monitor	xmlb05200.bin	n/a	
	Application	xmlp05200a.bin	n/a	
	Combined FPGA	lpfpga05200a.bin	n/a	
	Individual FPGA images		pbifsp2_05200a.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	3.24
			xppsp2_05200a.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	6.23
			xppoc_05200a.bin (POS interface modules)	6.22
			pbifoc_05200a.bin (POS interface modules)	3.06
			statsoc_05200a.bin (POS interface modules)	2.06
			pbifmrj_05200a.bin (24x1G and 48x1G modules)	3.25
			xppmrj_05200a.bin (24x1G and 48x1G modules)	6.24
			statsmrj_05200a.bin (24x1G and 48x1G modules)	0.09
			pbif8x10_05200a.bin (8x10G modules)	1.04
			xpp8x10_05200a.bin (8x10G modules)	3.08
		xgmacsp2_05200a.bin (2x10G and 4x10G modules)	0.15	
		xpp2x100_05200a.bin (2x100G modules)	2.20	
	Switch fabric modules	SBRIDGE	sbridge_05200a.mcs	6
High speed switch fabric modules	HSBRIDGE	hsbridge_05200a.mcs	16	

Brocade NetIron CES and NetIron Brocade NetIron CER devices

TABLE 29 Required images for a basic R05.2.00a software upgrade

Image description	Image name
Application - Multi-Service IronWare	ce05200a.bin
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin
fpga-pbif image	pbifmetro_05200a.bin

FIPS R05.0.00a images

FIPS enabled Brocade MLX Series and NetIron XMR devices

TABLE 30 Required images for a basic FIPS enabled upgrade to R05.2.00a

Required image	Image name	Signature file name
Combined application image for management modules	xm05200a.bin	xmr05200a.sig xmpl05200a.sig
Monitor image for management modules	xmb05200.bin	xmb05200.sig
Monitor image for interface modules	xmlb05200.bin	xmlb05200.sig
Boot image for management modules	xmprm05200.bin	xmprm05200.sig
Boot image for interface modules	xmplprm05200.bin	xmplprm05200.sig
Combined FPGA image for interface modules	lpfpga05200a.bin	lpfpga05200a.sig

C Required images for R05.2.00a

TABLE 31 FIPS enabled Multi-Service IronWare R05.2.00a image files

Hardware	Image type	Image name	Signature file name	Compatible version		
Management modules	Boot	xmprm05200.bin	xmprm05200.sig	n/a		
	Monitor	xmb05200.bin	xmb05200.sig	n/a		
	Application	xmr05200a.bin	xmr05200a.sig	n/a		
	Combined application	xm05200a.bin	xm05200a.sig	n/a		
	MBRIDGE	mbridge_05200a.xsvf	mbridge_05200a.sig	32		
	MBRIDGE32	mbridge32_05200a.xsvf (32-slot routers only)	mbridge32_05200a.sig	33		
Interface modules	Boot	xmlprm05200.bin	xmlprm05200.sig	n/a		
	Monitor	xmlb05200.bin	xmlb05200.sig	n/a		
	Application	xmlp05200a.bin	xmlp05200a.sig	n/a		
	Combined FPGA	lpfpga05200a.bin	lpfpga05200a.sig	n/a		
	Individual FPGA images		pbifsp2_05200a.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	pbifsp2_05200a.sig	3.24	
			xppsp2_05200a.bin (2x10G, 4x10G, and 20x1G Ethernet modules)	xppsp2_05200a.sig	6.23	
			xppoc_05200a.bin (POS interface modules)	xppoc_05200a.sig	6.22	
			pbifoc_05200a.bin (POS interface modules)	pbifoc_05200a.sig	3.06	
			statsoc_05200a.bin (POS interface modules)	statsoc_05200a.sig	2.06	
			pbifmrj_05200a.bin (24x1G and 48x1G modules)	pbifmrj_05200a.sig	3.25	
			xppmrj_05200a.bin (24x1G and 48x1G modules)	xppmrj_05200a.sig	6.24	
			statsmrj_05200a.bin (24x1G and 48x1G modules)	statsmrj_05200a.sig	0.09	
			pbif8x10_05200a.bin (8x10G modules)	pbif8x10_05200a.sig	1.04	
			xpp8x10_05200a.bin (8x10G modules)	xpp8x10_05200a.sig	3.08	
			xgmacsp2_05200a.bin (2x10G and 4x10G modules)	xgmacsp2_05200a.sig	0.15	
			xpp2x100_05200a.bin (2x100G modules)	xpp2x100_05200a.sig	2.20	
		Switch fabric modules	SBRIDGE	sbridge_05200a.mcs	sbridge_05200a.sig	6
		High speed switch fabric modules	HSBRIDGE	hsbridge_05200a.mcs	hsbridge_05200a.sig	16

FIPS enabled Brocade NetIron CES and Brocade NetIron CER devices

TABLE 32 Required images for a FIPS enabled upgrade to R05.2.00a

Required image	Binary image name	Signature Image name	Signature Filename on Flash
Application - Multi-Service IronWare	ce05200a.bin	ce05200a.sig	primary.sig
Boot and monitor image (for Brocade NetIron CER and Brocade NetIron CES devices, the boot and monitor images are the same)	ceb05100.bin	ceb05100.sig	monitor.sig, boot.sig
fpga-pbif image	pbifmetro_05200a.bin	pbifmetro_05200a.sig	pbifmetro.sig