SOFTWARE UPGRADE GUIDE

Extreme NetIron Software Upgrade Guide, 6.3.00a

Supporting NetIron OS 6.3.00a

9036141-00
March 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the 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.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

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.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
`Courier font`	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   NOTE
   You can modify your product selections or unsubscribe at any time.

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

Supported hardware and software

End of Support for ExtremeSwitching CES 2000 Series devices

Beginning with NetIron OS 6.3.00a and later, the ExtremeSwitching CES 2000 Series devices are not supported. Refer to the End of Sale and End of Support page for additional information.

The hardware platforms in the following table are supported by this release of this guide.

TABLE 1 Supported devices

ExtremeRouting XMR Series	ExtremeRouting MLX Series	ExtremeRouting CER 2000 Series
XMR 4000	MLX-4	CER 2024C
XMR 8000	MLX-8	CER-RT 2024C
XMR 16000	MLX-16	CER 2024F
XMR 32000	MLX-32	CER-RT 2024F
	MLXe-4	CER 2048C
	MLXe-8	CER-RT 2048C
	MLXe-16	CER 2048CX
	MLXe-32	CER-RT 2048CX
		CER 2048F
		CER-RT 2048F
		CER 2048FX
		CER-RT 2048FX

Supported software

For the complete list of supported features and the summary of enhancements and configuration notes for this release, refer to the *Extreme NetIron Release Notes*.

How command information is presented in this guide

Starting with Extreme NetIron 5.6.00, command syntax and parameter descriptions are removed from commands that are referenced in configuration tasks. To find the full description of a specific command, including all required and optional keywords and variables, refer to the *Extreme NetIron Command Reference* for your software release.

What's new in this document

This document describes the concepts and configuration of the upgrade and downgrade processes for NetIron.

> NOTE
> The NetIron 6.3.00 release (the image files and the documentation) is no longer available from the Extreme Portal. New software features introduced in release 6.3.00 are included in release 6.3.00a.

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks., Inc., as appropriate.

For the complete list of supported features and the summary of enhancements and configuration notes for this release, refer to the Extreme NetIron OS Release Notes.

TABLE 2 Document changes

Enhancement	Description	Described in
Added information on synchronizing MBRIDGE images	Added "Synchronizing MBRIDGE images between the active and standby management modules".	Synchronizing MBRIDGE images between the active and standby management modules on page 38
Updated the upgrade and downgrade considerations per SHA256 signature requirements.	Changed "Upgrade and downgrade considerations" section, Scenario 1 and Scenario 2.	Upgrade and downgrade considerations on page 17
Updated the release information to NetIron 6.3.00a and later releases.	Changed "06.3.00" to "6.3.00" and added "a and later releases" in the section titled, "Migration path to NetIron 6.3.00a and later releases". Changed "06.0.00" to "6.3.00" and added "a and later releases" in the section titled, "Upgrade and downgrade considerations".	Migration path to NetIron 6.3.00a and later releases on page 15 Upgrade and downgrade considerations on page 17
Updated the release information from "06.0.00" to "6.0.00 and later" releases.	Changed "06.0.00" to "06.0.00 and later" in the section titled, "General upgrade considerations". Changed "06.0.00" to "06.0.00 and later" in subsections in the section titled, "Software upgrades for Extreme MLX Series and NetIron XMR devices".	General upgrade considerations on page 19 R06.0.00 and later images on page 25 subsection in the section titled, "Software upgrades for Extreme MLX Series and NetIron XMR devices" Important memory information for an R06.0.00 (and later releases) upgrade on page 25 subsection in the section titled, "Software upgrades for Extreme MLX Series and NetIron XMR devices" Performing a basic upgrade on page 27 subsection in the section titled, "Software upgrades for Extreme MLX Series and NetIron XMR devices"
Updated the release information from "06.0.00" to "6.0.00 and later" releases.	Changed "06.0.00" to "06.0.00 and later" in subsections in the section titled, "Software Upgrades for Extreme NetIron CER Series and NetIron CES Series devices".	R06.0.00 and later images on page 43 subsection in the section titled, "Software Upgrades for Extreme NetIron CER Series and NetIron CES Series devices" Step 1 - Determining current image versions on page 44 in the section titled, "Software Upgrades for Extreme NetIron CER Series and NetIron CES Series devices"

TABLE 2 Document changes (continued)

Enhancement	Description	Described in
Updated the release information from "06.0.00" to "6.0.00 and later" releases.	Changed "06.0.00" to "6.0.00 and later" in the section titled, "Hitless OS upgrade support limitations".	Hitless OS upgrade support limitations on page 47
Updated the release information from "06.0.00" to "6.0.00 and later" releases.	Changed "06.0.00" to "6.0.00 and later" in the section titled, "Setting port auto-negotiation".	Setting port auto-negotiation on page 77

Important Upgrade Information for all Supported Devices

This chapter contains important information you will need to perform your Extreme NetIron software upgrade.

For additional upgrade information on the following topics, refer to Troubleshooting on page 79:

- Upgrading devices in MCT topologies on page 79
- Recovering from a failed upgrade on page 79

Migration path to NetIron 6.3.00a and later releases

Upgrade and downgrade considerations for NetIron 6.3.00a and later releases.

To establish an appropriate migration path from your current release of Extreme NetIron, consult your Extreme TAC representative (see the Preface of this document).

To upgrade to 6.3.00a and later releases, a multiple step process may be required. The multiple step upgrade process is not required for CER or CES.

Scenario 1

Customers running releases 05.9.00a, 05.6.00ga, 05.6.00h, 05.8.00e, 05.7.00e or subsequent releases can directly upgrade to NetIron 6.3.00a and later releases.

> NOTE
> If you are not running one of the releases listed above, you CANNOT directly upgrade to 6.3.00a and later releases.

Scenario 2

To upgrade from 05.6.00c or any later release (other than the images mentioned in Scenario 1), a two-step approach is required.

1. Upgrade to 05.9.00a or any of the following releases: 05.6.00ga, 05.6.00h, 05.8.00e, 5.7.00e or subsequent patch releases and reload the device.
2. Upgrade to NetIron 6.3.00a (and later releases). Reload the device.

Scenario 3

To upgrade to NetIron 6.3.00a and later from releases prior to R05.6.00c, a multiple step approach is required.

1. Upgrade to 5.9.00a or any of the following releases: 5.6.00ga, 5.6.00h, 5.8.00e or 5.7.00e and reload the device.
2. Upgrade again to the same image which was used in step 1 and reload the device again. This ensures that the device will have the SHA256 signatures on the device if they are needed, for example for LP Auto-upgrade.
3. Upgrade to NetIron 6.3.00a (and later releases), and reload the device.

Scenario 4

Use Scenario 4 if you want to use the following features specific to the NPB FPGA.

- VxLAN header stripping
- GTP de-encapsulation
- Packet Timestamping
- Source port labeling
- NVGRE stripping
- NetIron 6.3.00a (and later releases) UDA Enhancements

1. Upgrade to NetIron 6.3.00a (and later releases) using any of above scenarios based on the image from which the upgrade is being performed.
2. Reload the device again and verify that the system is up with NetIron 6.3.00a (and later releases).
3. Configure the **fpga-mode-npb** command and save the configuration.
4. Upgrade to the NetIron 6.3.00a NPB image using MLX_npb_06300a_mnf.txt and reload the device.
5. Make sure BR-MLX-10Gx20 and BR-MLX-100Gx2-CFP2 have NPB XPP images.
6. Verify the system. Check the output of the **show version** command and the **show flash** command to make sure the image versions are correct. Check the output of the **show module** command to make sure the line cards are not in Interactive state due to FPGA mismatch. Interactive state is an error state due to FPGA mismatch.

For example, the following output excerpts display sample command output used to verify the system.

Output example for the show version command

```
device# show version
SL M1: BR-MLX-MR2-M Management Module Active (Serial #: BVP0404J024, Part #: 60-1002374-06):
Boot     : Version 5.9.0T165 Copyright (c) 1996-2015 Brocade Communications Systems, Inc.
Compiled on Mar 19 2015 at 03:16:46 labeled as xmprm05900
(521771 bytes) from boot flash
Monitor  : Version 6.2.0T165 Copyright (c) 1996-2015 Brocade Communications Systems, Inc.
Compiled on Aug 17 2017 at 11:22:12 labeled as xmb06200
(546965 bytes) from code flash
IronWare : Version 6.3.0T163 Copyright (c) 1996-2015 Brocade Communications Systems, Inc.
Compiled on Nov 11 2018 at 02:06:22 labeled as xmr06300a
(10688855 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 37
1666 MHz Power PC processor 7448 (version 8004/0202) 166 MHz bus
512 KB Boot Flash (MX29LV040C), 128 MB Code Flash (MT28F256J3)
4096 MB DRAM INSTALLED
4096 MB DRAM ADDRESSABLE
Active Management uptime is 8 minutes 30 seconds
```

Output example for the show flash command

```
device# show flash
Active Management Module (Left Slot)
Code Flash - Type MT28F256J3, Size 128 MB
  o IronWare Image (Primary)
    Version 6.3.0T163, Size 10688855 bytes, Check Sum 8ed7
    Compiled on Nov 11 2018 at 02:06:22 labeled as xmr06300a
  o LP Kernel Image (Monitor for LP Image Type 0)
    Version 6.2.0T175, Size 573366 bytes, Check Sum faad
    Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200
  o LP IronWare Image (Primary for LP Image Type 0)
    Version 6.3.0T177, Size 9572536 bytes, Check Sum 42cd
    Compiled on Aug 25 2018 at 09:35:50 labeled as xmlp06300
  o Monitor Image
    Version 6.2.0T165, Size 546965 bytes, Check Sum b926
    Compiled on Aug 17 2017 at 11:22:12 labeled as xmb06200
  o Startup Configuration
```

```
    Size 246600 bytes, Check Sum 8caa
    Modified on 17:40:15 GMT+09 Mon Sep 10 2018
```

Output example for the show module command

```
device# show module
Module                                    Status                  Ports    Starting MAC
M1 (left ):BR-MLX-MR2-M Management Module  Active
M2 (right):BR-MLX-MR2-M Management Module  Standby(Ready State)
F1: NI-X-HSF Switch Fabric Module         Active
F2: NI-X-HSF Switch Fabric Module         Active
F3:
S1: NI-MLX-10Gx8-M 8-port 10GbE (M) Module  CARD_STATE_UP          8        0024.388a.4e00
S2: NI-MLX-10Gx8-M 8-port 10GbE (M) Module  CARD_STATE_UP          8        0024.388a.4e30
S3: BR-MLX-1GFx24-X 24-port 1GbE SFP Module CARD_STATE_UP          24       0024.388a.4e60
S4: BR-MLX-1GFx24-X 24-port 1GbE SFP Module CARD_STATE_UP          24       0024.388a.4e90
```

OpenFlow upgrade and downgrade

When downgrading the system from NetIron 6.3.00a (and later releases) to NetIron 05.8.00, if there are any VRF interfaces that are enabled with OpenFlow, some unexpected IFL entries will be seen after moving to R05.8.00. These unexpected IFL entries may affect the L3VPN/6VPE traffic.

Extreme recommends removing OpenFlow from the VRF interfaces before downgrading the router to R05.8.00.

Hitless Upgrade support

Hitless Upgrade from any release to NetIron 6.3.00a is NOT supported.

Upgrade and downgrade considerations

Upgrade and downgrade scenarios for NetIron 6.3.00a and later releases, and Network Packet Broker.

To upgrade to 6.3.00a and later releases, a multiple step upgrade process may be required for MLXe and XMR. The multiple step upgrade process is not required for CER or CES.

Scenario 1

Customers running releases 6.0.00, 5.9.00a, 5.6.00ga, 5.6.00h, 5.8.00e and 5.7.00e can directly upgrade to 6.3.00a and later releases if SHA256 signatures exist on the manage module flash.

Procedure to verify SHA256 Signatures:

1. Log into the MLX router management module.
2. Enter **dir** to list the `/flash/` directory.

```
    #dir
    Directory of /flash/

    04/26/2018 21:55:27                  1  $$snmp_boots
    02/28/2018 14:45:57              1,740  $$sshdsaclient.key
    02/28/2018 14:45:57                643  $$sshdsapub.key
    07/11/2016 22:21:54                716  $$sshdsspub.key
    07/12/2016 16:15:08              1,564  $$sshrsahost.key
    07/10/2018 18:36:17              3,588  $$user_profile
    07/17/2018 22:19:20            660,145  ___mbridge
    06/15/2018 18:49:58                120  boot-parameter
    04/26/2018 22:55:28              3,642  dhcpsnoop_data
    07/17/2018 21:58:32                460  fips_public_key.crt
    07/14/2018 04:04:38            524,288  lp-boot
    07/17/2018 21:29:17            524,288  lp-boot-0
    07/17/2018 21:58:33                256  lp-mon.sig
    07/17/2018 22:03:14            571,513  lp-monitor-0
    07/17/2018 21:58:48                256  lp-pri.sig
```

```
07/17/2018 22:05:19              9,552,493  lp-primary-0
07/17/2018 21:59:02                    256  lpfpga.sig
07/17/2018 21:58:32                  2,987  manifest
07/17/2018 21:58:32                    256  manifest.sig
07/17/2018 22:02:56                    256  mbridge.sig
07/17/2018 22:03:11                546,489  monitor
07/17/2018 21:58:32                    256  monitor.sig
07/17/2018 22:04:25             10,635,252  primary
07/17/2018 21:58:33                    256  primary.sig
07/17/2018 22:40:42                 92,026  startup-config

               25 File(s)       23,123,747 bytes
                0 Dir(s)       103,809,024 bytes free
```

3. If the `256 primary.sig` file is listed, then you can directly upgrade to 6.3.00a (Target Version) and later releases.
4. If the `256 primary.sig` file is not listed, then you must use Scenario 2.

Scenario 2

To upgrade from 5.6.00c or any later release (other than the images mentioned in Scenario 1), the following steps are required.

1. Upgrade to 5.9.00x or any of the following releases: 5.6.00x, 5.6.00h, 5.8.00x or 5.7.00e, and reload the device.
2. Verify that SHA256 signatures are present using the "Procedure to verify SHA256 Signatures" in Scenario 1. If the `256 primary.sig` file is not listed, repeat steps 1 and 2 until the file is listed.
3. Upgrade to 6.3.00a (and later releases). Reload the device.

Scenario 3

To upgrade to 6.3.00a (and later releases) from releases prior to R05.6.00c, a multiple step approach is required.

1. Upgrade to 5.9.00a or any of the following releases: 5.6.00ga, 5.6.00h, 5.8.00e or 5.7.00e and reload the device.
2. Upgrade again to the same image which was used in step 1 and reload the device again. This ensures that the device will have the SHA256 signatures on the device if they are needed, for example for LP Auto-upgrade.
3. Upgrade to 6.3.00a (and later releases) and reload the device.

OpenFlow upgrade/downgrade

When downgrading the system from R06.3.00a to R05.8.00, if there are any VRF interfaces which are enabled with OpenFlow, some unexpected IFL entries will be seen after moving to R05.8.00. These unexpected IFL entries may affect the L3VPN/6VPE traffic.

Extreme recommends removing OpenFlow from the VRF interfaces before downgrading the router to R05.8.00.

Hitless upgrade

Hitless upgrade support Hitless Upgrade from any release to 6.3.00a is NOT supported.

Upgrade to 6.3.00a for the Network Packet Broker (NPB) global setting

To upgrade to 6.3.00a and later releases for the NPB global setting, a multiple step approach is required.

1. Upgrade to NetIron R06.3.00a using the NPB manifest file.
2. Reload the system.
3. Configure the NPB global setting using the **fpga-mode-NPB** command.
4. Reload the system.

Upgrading a single slot on a device

If you are upgrading a single slot on your hardware device, you must perform a signature verification for each slot. NetIron OS does not store the files in the management processor for a single slot upgrade. By default, the verification is performed only when all slots have been upgraded.

General upgrade considerations

NOTE
The upgrade process for R05.2.00 and later releases is different than for the releases prior to R05.2.00. The upgrade instructions documented here must be followed to upgrade a system from a pre R5.2.00 release to R5.2.00 or later releases. If you need assistance with the upgrade process, please contact Extreme Support.

The following general considerations apply to upgrades to NetIron 6.0.00 and later releases.

When upgrading to NetIron 6.0.00 and later releases from NetIron 5.9.00a, 5.8.00e, 5.7.00e, 5.6.00h, or 5.6.00ga, a direct upgrade can be performed.

When upgrading to NetIron 6.0.00 and later releases from releases prior to NetIron 5.6.00c, a multiple step approach is required.

1. Upgrade to any of these NetIron releases: 5.9.00a, 5.8.00e, 5.7.00e, 5.6.00h, 5.6.00ga. Reload the device.
2. Upgrade again to the same image which was upgraded to in step 1 and reload the device again. This ensures that the device will have the SHA256 signatures on the device if they are needed, for example for LP Auto-upgrade.
3. Upgrade to NetIron 6.0.00 (and later releases) and reload the device.

To upgrade from NetIron 5.6.00c or any later release other than the images mentioned above, upgrade to NetIron 5.9.00a and then upgrade to NetIron 6.0.00 and later releases.

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

NOTE
Before you begin your R06.0.00 (and later releases) upgrade, you must clear enough code flash memory for the upgrade to be successful. Refer to Important memory information for an R06.0.00 (and later releases) upgrade on page 25.

- Because of code flash memory considerations, software versions R05.2.00 and later releases operate using a single copy of each image instead of primary and secondary images. R05.2.00 and later releases only support a single (primary) image on each module.
- 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 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 images unless you are explicitly instructed to do so in the upgrade instructions for the version you are using.
- Hitless OS upgrades are only 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 Hitless OS Upgrade for all Supported Devices on page 47.
- Simplified Upgrades are only supported for upgrades from MultiService IronWare R05.3.00 to a higher release. For more information about Simplified Upgrades, refer to Simplified Upgrade and Auto Upgrade on page 51.
- The combined FPGA image is not supported in releases prior to MultiService IronWare R04.1.00.

- 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 version using the **show version** command.
- If you are currently running MultiService IronWare 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.
- Beginning with MultiService IronWare R05.3.00, all types of POS modules are not supported.
- Beginning with MultiService IronWare R05.3.00, SNTP is not supported. When upgrading to R05.3.00, all SNTP configurations will be lost. SNTP functionality is replaced with NTP (Network Time Protocol).
- When upgrading FPGA images on a Line Card, a power cycle of the Line Card is required using either the MP system **reload** or **power-off lp** and **power-on lp** commands. The **lp boot sys flash** command does not perform a Line Card power cycle and is not sufficient to upgrade the FPGA images.
- The use of the "wait-for-all-cards" configuration in MultiService IronWare R05.3.00 may cause ports on any 1G module to stay down after boot-up, even if configured to be enabled. To avoid such an occurrence, it is recommended that the "wait-for-all-cards" configuration be removed from the startup-config prior to reloading the router with R05.3.00 code. For more information, refer to Troubleshooting on page 79.
- It is recommended to start a log file to capture the upgrade process for troubleshooting purposes if an unexpected event occurs.
- A two cycle upgrade is required when upgrading between SHA256 signature packages to non-SHA256 signature packages.

  NOTE
  Refer to the Federal Information Processing Standards and Common Criteria Guide for more information when upgrading from non-SHA256 signatures to SHA256 signature packages or downgrading from SHA256 signature to non-SHA256 signature packages.

- When upgrading from a release that does not support SHA256 signatures to a release that does, please upgrade twice to the same release as follows. First upgrade to the release that supports SHA256 signatures. Reload the device. Then upgrade again to the same release that supports SHA256 signatures, and reload the device again. This ensures that the device will have the SHA256 signatures on the device if they are needed, for example for LP Auto-upgrade.
- Beginning with NetIron 6.0.00a the option is available to install the Network Packet Broker (NPB) FPGA manifest file. Refer to the NetIron 6.0.00a Release Notes for installation information and limitations.

  NOTE
  There is specific case where NetIron 5.8.00b and NetIron 6.0.00 releases will not interoperate with each other when a default configuration is used in **ikev2 auth- proposal** to setup an IPsec tunnel. The default value for IKEv2 authentication proposal has changed in the NetIron 6.0.00 release. In NetIron 6.0.00 the pre _shared key is the default method, with the pre_shared key set to default value **def-ike-pre-shared-password**. To continue IKEv2 authentication interoperability between NetIron 5.8.00b and NetIron 6.0.00, you will need to ensure that the same IKEv2 authentication is configured on both nodes.

To prevent loss of interoperability:

1. Before upgrading:

EITHER

Configure non-default, IKEv2 authentication on both nodes for the IPsec tunnel.

OR

On each NetIron 5.8.00b node, change the authentication method to the pre _shared key with the key set to value **def-ike-pre-shared-password**.

2. Save the configurations.

3. Upgrade to NetIron 6.0.00.

General downgrade considerations

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

- Extreme MLXe routers must not be downgraded to software releases prior to R05.0.00c.
- MLX Series and XMR Series 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.
- MLX Series and XMR Series 4x10G-X modules (BR-MLX-10Gx4-X, BR-MLX-10Gx4-X-ML) must not be downgraded to versions prior to R05.1.00.
- MLX Series 8x10G modules (NI-MLX-10Gx8-M, NI-MLX-10Gx8-D) must not be downgraded to versions prior to R05.0.00b.
- XMR Series 8x10G modules (BR-MLX-10Gx8-X) must not be downgraded to versions prior to R05.2.00.
- MLX Series and XMR Series 100G modules (BR-MLX-100Gx2-X, BR-MLX-100Gx1-X) must not be downgraded to versions prior to R05.2.00.
- MLX-32 devices must not be downgraded to versions prior to R03.6.00.
- CER 2000 Series devices must not be downgraded versions prior to R04.1.00a software.
- A two cycle downgrade/upgrade is required when downgrading between SHA256 signature packages to non-SHA256 signature packages. Generally , NI releases prior to 5.6 patch C (but not 5.6 patch AA) do not support SHA256 signatures.
- When downgrading from a release that does support SHA256 signatures to a release that does not, please downgrade twice to the same release as follows. First downgrade to the release that does not support SHA256 signatures. Reload the device. Then downgrade again to the same release that does not support SHA256 signatures, and reload the device again. This ensures that the device will have non-SHA256 signatures on the device after downgrade if they are needed, for example for LP Auto-upgrade.
- When downgrading from NetIron 6.2.00 NPB software image to NetIron 6.1.00 or 6.0.00a (non-NPB image), the administrator must ensure that the device is rebooted after flashing the NetIron 6.1 or 6.0a image and the device has booted with NetIron 6.1 or 6.0a software version and then execute the **no fpga-mode-npb** command. The administrator must refrain from configuring **no fpga-mode-npb** while device still runs on NetIron 6.2 NPB image as it would cause the uda-offsets (which are specific to UDA ACL feature) configured on the interfaces to change

  NOTE

  Downgrade from SHA256 signature to non-SHA256 signature packages requires two downgrade cycles to update the signature files from SHA256 signatures for LP Auto-upgrade to use the non-SHA256 signatures for manifest file signature check. When downgrading the following warning message may be seen:

```
Failed to rename manifest_tmp.sig into manifest.sig
```

Special upgrade information for Extreme MLXe devices

The following general considerations apply to upgrade MLX Series devices:

- Extreme MLXe devices require a minimum software release of R05.0.00c.

- In rare circumstances, you may receive management modules with 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 an Extreme 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 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 MLX Series or XMR Series 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.

NOTE
Starting in R06.0.00a two combined FPGA images will be available for download: the standard (MAIN) FPGA image and the Network Packet Broker (NPB) FPGA image. The Network Packet Broker FPGA image version is specific to the functionality of the Network Packet Broker.

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 of 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 *MultiService Ironware 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 26.

Software Upgrades for Extreme MLX Series and NetIron XMR devices

This chapter describes how to upgrade your Multi-Service IronWare software to R06.0.00 and later releases.

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

Before you begin your upgrade, read Important Upgrade Information for all Supported Devices on page 15 to make sure your system does not have special upgrade requirements.

R06.0.00 and later images

Refer to the relevant version of the Extreme NetIron Release Notes for all R06.0.00 and later images.

NOTE
When upgrading Multi-Service Ironware, follow the manifest upgrade to ensure all required files are upgraded. Boot upgrade is not part of the manifest upgrade. Compatible boot images for Multi-Service IronWare R06.0.00 and later releases include 05900 and 05800 versions. Although not required, it is recommended to use the most current version of the boot image.

NOTE
If the manifest upgrade is not followed, check the boot image for management, interface modules and the monitor image for compatibility.

For a list of all images for Multi-Service IronWare R06.0.00 and later, refer to the relevant version of the Extreme *NetIron Release Notes*.

Performing a patch upgrade

For patch releases, in most cases, boot and monitor images do not need to be upgraded. Refer to the *Extreme NetIron Release Notes* for information about which image must be upgraded for a specific patch.

NOTE
Starting in R06.0.00a two combined FPGA images will be available for download: the standard (MAIN) FPGA image and the Network Packet Broker (NPB) FPGA image. The Network Packet Broker FPGA image version is specific to the functionality of the Network Packet Broker.

Important memory information for an R06.0.00 (and later releases) 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 R06.0.00 (and later) to the standby management module during the course of the upgrade process.

NOTE
Because of code flash memory considerations, R05.2.00 and later software operates using a single copy of each image instead of primary and secondary images. R05.2.00 and later supports only a single (primary) image on each module.

NOTE
You should not need to remove any other files then 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

R05.2.00 and later only support a single image on each module. 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 lp application image by entering the following command.

   delete lp-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

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.

```
device# dir
Directory of /flash/
01/11/2011    03:18:42    2 $$snmp_boots
09/30/2009    03:47:50    5,201 $$sshdsspub.key
06/15/2011    21:19:04    660,145___mbridge
12/07/2010    22:16:23    139 boot parameter
06/15/2011    21:20:00    524,288 lp-monitor-0
06/15/2011    21:07:44    4,950,939 lp-primary-0
06/15/2011    21:19:28    524,053 monitor
06/15/2011    21:08:37    6,986,237 primary
06/20/2011    17:11:42    620,225 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

R05.2.00 and later support only a single image on each module. To remove secondary application image files from each interface module, perform the following steps:

1. Enter the **show module** command and note the slots the interface modules are installed into for the device.
2. 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@
device#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>
...
```

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

```
LP-2# dir
Directory of /flash/
    File Name    Size    Chksum
    PBIF    112    81ed
    XPP    112    7ff7
    boot    524288    6c2b
    monitor    524288    fd4a
    primary    4950939    df45
     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 the 6.0.00 and later *NetIron Release Notes*, 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 Software Upgrades for Extreme MLX Series and NetIron XMR devices on page 25 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 28.
- Step 2 - Upgrading the management module monitor image on page 30.
- Step 3 - Upgrading the management module boot image on page 30.
- Step 4 - Upgrading the combined application image on management modules on page 31.
- Step 5 - Upgrading boot and monitor images on interface modules on page 31.
- Step 6 - Upgrading interface modules using the combined FPGA image on page 32.
- Step 7 - Performing supplemental image upgrades (as needed) on page 33.
- Step 8 - Performing an image coherence check on page 33.
- Step 9 - Reloading the management module on page 34.

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 installed image versions to the compatible image version numbers listed in the 6.0.00 and later *NetIron Release Notes*.

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.

```
device# 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
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

```
device# 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
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
```

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 *xxxxx* **.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** *xxxxx.* **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 *xxxxx* **. 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* **xmprm** *xxxxx* **.bin boot**
   - – Using the flash card:

   copy [**slot 1 | slot 2]flash xmprm***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 and later software operates using a single copy of each image instead of primary and secondary images. R05.2.00 and later only supports a single (primary) image on each module.

NOTE
Do not use the **copy tftp flash** command when upgrading the Combined Application Image (for example: **xm05600.bin**) or the system will only upgrade the Management Module Application image and will not upgrade the Interface Module Application image.

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 one of the following commands.
   - – Using SCP on a remote client:

   C:> scp xm *xxxxx.* **bin** *user@device-IpAddress:* **image: [primary | secondary]**
   - – Using TFTP at the Privileged EXEC level of the CLI:

   copy tftp image *tftp-srvr* **xm** *xxxxx* **.bin** [**primary** |**secondary**] [**delete-first**]
   - – Using the flash card

   copy [**slot 1** |**slot 2**] **image xm***xxxx***.bin** [**primary** | **secondary**] [**delete-first]**

   The **primary** option copies the files to the primary image on the management module.

   The **secondary** option copies the files to the secondary image on the management module.

   The **delete-first** option automatically deletes the existing primary or secondary flash images before installing the new images.
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
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***xxxxx***.bin** *user@device-IpAddress:***lp:monitor** :[**all** / *slot-number*]

   C:> **scp xmlprm***xxxxx***.bin** *use>@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** *xxxxx* **.bin monitor** [**all** |*slot-number*]

   copy tftp lp *tftp-srvr* **xmlprm** *xxxxx* **.bin boot** [**all** |*slot-number*]
   - – Using the flash card

   copy [**slot 1** |**slot 2**] **lp xmlb***xxxx***.bin monitor** [**all** |*slot-number*]

   copy [**slot 1** | **slot 2**] **lp xmlprm***xxxx***.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.

NOTE
Before you upgrade the FPGA code on the line cards, change the preforwarding timer to 1200 milliseconds (1.2 seconds). The value needs to be changed on all the switches in the MRP ring. For more information, refer to the **Metro Ring Protocol** chapter of the *Extreme NetIron Layer 2 Switching Configuration Guide*.

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***xxxxx***.bin***user@device-IpAddress***:lp:fpga-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** *xxxxx* **.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:

   ```
   Copying 1st image (PBIF - Ethernet) to slot(s) 6, 8 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 supplemental image upgrades (as needed)

This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to the images and versions listed in the current version of the *Extreme NetIron Unified Release Notes*. If your system image versions differ from those listed in the table, you will need to upgrade them using the following sections:

- Upgrading MBRIDGE or MBRIDGE32 images on management modules
- Upgrading the SBRIDGE image on 32-slot devices
- Upgrading the HSBRIDGE image on 32-slot devices

Step 8 - 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.

This example displays a mismatch between the FPGA versions on the active MM and standby MM.

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

Warning: Mbridge FPGA mismatch between active(37) and standby(36) module
Done.
device#
```

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.

   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. This example displays warnings about application conflicts.

```
device# 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 9 - Reloading the management module

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

> NOTE
> When upgrading FPGA images on a Line Card, a power cycle of the Line Card is required using either the MP system **reload** or **power-off lp** and **power-on lp** commands. The **lp boot sys flash** command does not perform a Line Card power cycle and is not sufficient to upgrade the FPGA images.

Before reloading the management module, use the **write memory** command to save the current configuration.

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)

For example:

```
device# reload
Checking for coherence...
Done.
Are you sure? (enter 'y' or 'n'): y
Halt and reboot
```

boot system flash [**primary**]

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 Recovering from a failed upgrade on page 79.
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.

Extreme MLX Series and NetIron XMR supplemental upgrade procedures

The following chapter describe additional upgrade procedures that may be required to upgrade individual images. To determine whether you need to upgrade these images, refer to the Extreme *NetIron Release Notes*.

NOTE
Starting in R06.0.00a two combined FPGA images will be available for download: the standard (MAIN) FPGA image and the Network Packet Broker (NPB) FPGA image. The Network Packet Broker FPGA image version is specific to the functionality of the Network Packet Broker.

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 the *Extreme NetIron Release Notes*.

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***xxxx*.**xsvf***user@device-IpAddress*:**mbridge**
   - Using TFTP at the Privileged EXEC level of the CLI:

     copy tftp mbridge *tftp-srvr* **mbridge _** *xxxx* **.xsvf**
   - Using the flash card:

     copy [**slot 1** |**slot 2**] **mbridge mbridge_***xxxx*.**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.

NOTE
Always use TELNET on the MLX-32 chassis (instead of SSH). PROM write operations consume substantial CPU cycles, starving other tasks such as SSH. The end result includes timeouts within affected tasks. TELNET does not have similar issues (such as hello exchanges) and hence is not impacted.

Synchronizing MBRIDGE images between the active and standby management modules

This procedure describes how to synchronize mismatches of mbridge images between the active and standby MR or MR2 management modules in the following situations:

- A standby module could be inserted fresh from manufacturing into a network with higher version of mbridge installed.
- A standby module could be moved from an existing system into another system (migration) with a different version.

Both these cases could lead to an mbridge mismatch between the active and standby management modules.

Once the active management module declares that the standby is in sync, you can use the **reload** command to reload the entire node to synchronize MBRIDGE images between the active and standby management modules. However, if you do not want to reload the entire system node and want to upgrade the standby MP only to the more recent active MP, then follow these steps:

1. Rconsole into the standby MP by entering the **rconsole standby** command.
2. From the standby MP, enter into MP-OS mode by typing <ctrl-y> m and then <enter> (ctrl-y together, m by itself, and then enter).
3. From MP-OS mode, enter the **mbridge update** command and wait until the update is complete.
4. From MP-OS mode, enter the **reset** command.
   The following example of synchronizing MBRIDGE images resets the standby and comes up with the same version as active:

```
SSH@mlx16-1#rconsole standby
Remote connection to standby established
Press CTRL-X to disconnect it--- Standby Management ---
--- Standby Management ---
--- Standby Management ---
--- Standby Management ---
--- Standby Management --- <ctrl-y>  m   <enter>
MP-2 OS>mbridge ?
reload           Reload Mbridge
update           Update Mbridge
MP-2 OS>mbridge update
...
MP-2 OS> reset
```

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 the*Extreme NetIron Release Notes*.

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_***xxxx***.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_** *xxxx* **.mcs sbridge** [**all** |*slot-number*]
   - Using the flash card:

     copy [**slot 1** |**slot 2**] **snm 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.
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 the *Extreme NetIron Release Notes*.

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

NOTE
This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to the *Extreme NetIronRelease Notes*.

NOTE
Extreme recommends using the combined FPGA image to simplify the FPGA image upgrade procedure.

NOTE
When upgrading FPGA images on a Line Card, a power cycle of the Line Card is required using either the MP system '**reload** ' or '**power-off lp** ' and '**power-on lp** ' commands. The '**lp boot sys flash** ' command does not perform a Line Card power cycle and is not sufficient to upgrade the FPGA images.

NOTE
Before you upgrade the FPGA code on the line cards, change the preforwarding timer to 1200 milliseconds (1.2 seconds). The value needs to be changed on all the switches in the MRP ring. For more information, refer to the **Metro Ring Protocol** chapter of the *Extreme NetIron Switching Configuration Guide*.

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.binuser@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* [**all** |*module-type*] [**force-overwrite**]

   Specify the *fpga-image-namexxxx.bin* of the FPGA file you are copying, for example pbifsp2_05700.bin, xppsp2_05700.bin, etc. For a complete list of individual FPGA file names, refer to the *Extreme NetIron Release Notes*.

   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 Extreme NetIron CER Series and NetIron CES Series devices

This chapter describes how to upgrade software on CER 2000 Series and CES 2000 Series devices. The procedures described are identical for all models, except where indicated.

NOTE
The software described in this section applies only to the CER 2000 Series and CES 2000 Series devices. You cannot use this software on other Extreme devices.

R06.0.00 and later images

Refer to the latest version of the Extreme NetIron Release Notes for all R06.0.00 and later images.

NOTE
When upgrading Multi-Service Ironware, follow the manifest upgrade to ensure all required files are upgraded. Boot upgrade is not part of the manifest upgrade. Compatible boot images for Multi-Service IronWare R06.0.00 and later include 05900 and 05800 versions. Although not required, it is recommended to use the most current version of the boot image.

NOTE
If the manifest upgrade is not followed, check the boot and monitor image for compatibility.

Performing a patch upgrade

Refer to the latest version of the Extreme NetIron Release Notes 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.

Before you begin your upgrade, read Important Upgrade Information for all Supported Devices on page 15 to make sure your system does not require special upgrade steps.

Upgrading Multi-Service IronWare software for Extreme NetIron CES and CER devices requires an upgrade of the combined application image, boot image, and monitor images.

This upgrade requires the following steps:

- Step 1 - Determining current image versions on page 44
- Step 2 - Upgrading the application image on page 45
- Step 3 - Upgrading the fpga-pbif on page 45

- Step 4 - Upgrading monitor and boot image on page 45
- Step 5 - Reboot the device on page 46

Step 1 - Determining current image versions

Before you upgrade the images on a CER 2000 Series or CES 2000 Series 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 in R06.0.00 and later images on page 43. Upgrade any image versions that do not match.

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

```
device#show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Code Flash - Type MT28F256J3, Size 64 MB
  o IronWare Image (Primary)
    Version 5.3.0T183, Size 14385657 bytes, Check Sum e848
    Compiled on Jan 20 2012 at 18:56:08 labeled as ce05300
  o Monitor Image
    Version 5.3.0T185, Size 447585 bytes, Check Sum 58c7
    Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300
  o Startup Configuration
    Size 6002 bytes, Check Sum cc8a
    Modified on 19:50:20 GMT+00 Fri Jan 27 2012
Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 5.3.0T185, Size 447585 bytes, Check Sum 58c7
    Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

show version command output

```
device#show version
System: NetIron CER (Serial #: K40533F00H,  Part #: 40-1000372-04)
License: RT_SCALE, ADV_SVCS_PREM (LID: mJFKIIhFFj)
Boot     : Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.
Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300
(447585 bytes) from boot flash
Monitor  : Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.
Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300
(447585 bytes) from code flash
IronWare : Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.
Compiled on Jan 20 2012 at 18:56:08 labeled as ce05300
(14385657 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000d
Extended route scalability
PBIF Version: 0x56
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
System uptime is 1 minutes 37 seconds
device
```

NOTE
Upgrading the legacy NetIron CES and NetIron CER devices to R05.5.00 is a two step process now. First the application image has to be installed. After the device is on R05.5.00 application image, the corresponding PBIF image can be installed.

Step 2 - Upgrading the application image

To upgrade the combined application image (primary or secondary) for CER 2000 Series or CES 2000 Series 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***xxxx***.bin***user@device-IpAddress:***flash:** [**primary**]
   - – Using TFTP at the Privileged EXEC level of the CLI:

   copy tftp flash *tftp-srvr* **ce** *xxxx* **. bin** [**primary**]
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 Extreme NetIron CER or Extreme NetIron CES device, perform the following steps.

1. Place the pbifmetro_<XXXX>.bin file on a tftp server.

   NOTE
   This command must be entered from the console. Telnet, SSH and SCP are not supported.

2. Copy the fpga-pbif by entering the following command.
   - – 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 - Upgrading monitor and boot image

NOTE
CER 2000 Series or CES 2000 Series 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***xxxx*.**bin***user@device-IpAddress:***flash: [boot | monitor]**
   - Using TFTP at the Privileged EXEC level of the CLI:

   copy tftp flash *tftp-srvr* **ceb** *xxxx* **. 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.

Step 5 - 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**]
2. After the device finishes booting, enter the **show version** command, and verify that the device is running the new software image version.

If your upgrade fails, for recovery information refer to Recovering from a failed upgrade on page 79.

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

Hitless OS upgrade is not supported for any release to 06.0.00 and later releases.

Hitless OS Upgrade is not supported from any major release to another major release. For example, an upgrade from 5.8.00x or 5.9.00x to 6.0.00x is not supported.

Hitless OS Upgrade is not supported to 6.0.00a.

NOTE
Starting in R06.0.00a two combined FPGA images will be available for download: the standard (MAIN) FPGA image and the Network Packet Broker (NPB) FPGA image. The Network Packet Broker FPGA image version is specific to the functionality of the Network Packet Broker. Hitless OS Upgrade is not supported for R06.0.00a .

NOTE
Refer to the Release Notes for the specific version being upgraded before performing an upgrade. The Release Notes provide specific upgrade information and limitations for each release.

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.
- 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 3 lists supported and unsupported protocols and features for Hitless OS Upgrade.

TABLE 3 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: MRP STP RSTP VSRP	All MPLS features
Layer 3 protocols IGMP PIM OSPF BGP IS-IS	IPv4 and IPv6 multicast snooping
Static IP routes	IPv6 multicast routing
Layer-3 forwarding	VLAN translation
GRE tunnels	Policy-based routing
ACLs (the following ACLs continue to function but ACL counters are reset) • Layer 2 ACLs • IPv4 ACLs • IPv6 ACLs • IP Receive ACLs	FPGA upgrades VRRP and VRRP-E All VPN features MCT (Multi-chassis trunking) Network management to the device: SSH Telnet SNTP HTTP/HTTPS sFlow (interface modules only) Ping Traceroute Syslog messages are cleared SNMP and SNMP trap DNS DHCP AAA ERP (G.8032)Management VRF ToS-based QoS
IPv4 and Layer-2 ACL-based traffic policing	
Traffic policing	
UDLD	
LACP	
BFD	
802.1ag over VLANs	
IPv4 multicast routing	

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.

NOTE
If using an MR-2 module during a hitless upgrade an error message may begin to be displayed. This message should be ignored as it has no impact.

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 and 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 (for example, 05.3.00 to 05.3.00a) but are not supported for upgrades from one major release to another (for example 05.2.xx to 05.3.xx). Please refer to Hitless OS upgrade support limitations on page 47 for a list of releases that do not support Hitless Upgrade.

Some features and protocols are not supported for hitless upgrade. Before you perform a hitless upgrade, refer to Special considerations for Hitless OS Upgrade on page 47 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.

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

1. Copy the Multi-Service IronWare software images to the primary and secondary flash on the active and standby management modules and on interface modules.

   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**] | **lp** [**primary**]

   The **mp** parameter specifies that the image will be copied to the management module.

   The **lp** parameter specifies that the image will be reloaded to the interface module.

Simplified Upgrade and Auto Upgrade

This chapter describes how to upgrade your MultiService IronWare software using a single command, **copy tftp system manifest** . Before beginning your upgrade, refer to the appropriate chapters in this document for your device to make sure your system does not have special upgrade requirements.

NOTE
The Simplified Upgrade feature is available only when upgrading from R05.3.00.

Simplified Upgrade

Simplified Upgrade is a single operation that performs a full system upgrade of all the images. It can be as simple as one command from the CLI or one set-request operation from the SNMP. Prior to R05.3.00, several commands were required to upgrade your system. That method is still supported as described in the appropriate chapter for your device, however using the **copy tftp system** command with the new all images and manifest parameters introduced in R05.3.00, you can upgrade your system by issuing only one command.

In this release, the process will be optimized by introducing a version-check of the images to determine whether it is necessary to download/upgrade the image or not.

This simplified upgrade method greatly reduces the possibility of having incompatible interface modules due to incompatible image versions.

The command can be issued to download images from either of the following:

- TFTP server, as described in Upgrading the software using a TFTP server on page 55
- auxiliary storage device, as described in Upgrading the software using an auxiliary storage device on page 56

Use the all images parameter to upgrade the management and interface boot, monitor, and application images, as well as all interface and management FPGA images. Since many of these images are not required to be upgraded for each release and doing so can be time consuming, you can upgrade the management and interface monitor and application images, as well as the combined FPGA images only by omitting the all images parameter.

The default behavior is that the all images parameter is not specified.

NOTE
Management and interface boot images and individual boot images are generally not required to be upgraded and customers are not recommended to upgrade them, unless it is explicitly stated otherwise in release notes. Copying management interface FPGA images may temporarily affect time-sensitive protocols.

NOTE
For simplified upgrades on the NetIron CES and NetIron CER devices, the pbif_mero installation in simplified upgrade will fail and device will need to be reloaded. After all images are installed using Simplified upgrade, the pbif will need to be installed manually, and the device will need to be reloaded again.

NOTE

For a simplified upgrade from R05.6.00d to R05.7.00a, b, or c, the boot image is not upgraded as part of the manifest file due to it not being a necessary upgrade. The 5.6.00 boot image is compatible with the 5.7.00 version. When a **show version** is run on the Extreme MLX device, it will show the boot image as version 5.6.00, but the Extreme MLX device will be fully functional, and have the full update of 5.7.00c. You may still choose to manually upgrade to the R05.7.00 boot image. Both use cases are acceptable and will function properly on the Extreme MLX device.

Extreme NetIron XMR and MLX Series single-command (full-system) upgrade

There is no change in the syntax for the full-system upgrade; however, the expected behavior for the keyword "all-images" has changed.

Syntax: copy tftp system [all-images] <server-ip-address> manifest <File name> [lp-sec | mp-sec | secondary]

Syntax: copy <slot1 | slot2> system [all-images] manifest <File name> [lp-sec | mp-sec | secondary]

NOTE

Boot images are not included in the upgrade process for systems running Multi-Service IronWare Release 05.6.00d and later when the "all-images" option is used. The optional keyword "all-images" specifies to include only the MP FPGA images (MBRIDGE/MBRIDGE32 and SBRIDGE/HSBRIDGE).

Extreme NetIron CER and NetIron CES single-command (full-system) upgrade

NOTE

Boot images are not included in the upgrade process for systems running Multi-Service IronWare Release 05.6.00d and later when the "all-images" option is used. The "all-images" optional keyword is available in *Multi-Service IronWare R05.6.00d* and earlier versions only.

Syntax: copy tftp system [all-images] <server-ip-address> manifest <File name> [secondary]

Step 1: Download Manifest file and Validation

NOTE

While the simplified upgrade is in progress, CLI commands or SNMP set-requests that initiate a TFTP download are rejected.

When you issue the **copy tftp system** command using the manifest parameter, the first step the system performs is to download the digital signature file associated with the manifest file, download the manifest file and perform a signature check. This ensures the manifest file download is indeed created by Extreme, and not modified by others.

Step 2: Download File Images

Next, the system upgrades the system file images. The file images upgraded depend on how you enter the command. If you use the manifest and all images parameters, the files are upgraded in the following sequence:

- management module Boot image
- interface module Boot image
- management module Monitor image

- interface module Monitor image
- management module Application image
- interface module Application image
- Bundled FPGA image for all interface modules
- MBRIDGE (or MBRIDGE32 for 32-slot chassis)
- SBRIDGE or HSBRDGE image (for 32-slot chassis only)

If you do not use the all images parameter, the files are upgraded in the following sequence:

- management module Monitor image
- interface module Monitor image
- management module Application image
- interface module Application image
- Bundled FPGA image for all interface modules

Depending on the type of management module (MR or MR2) in the system, the system follows different behavior in downloading and installing the images.

Systems with MR management modules

In systems with MR management modules, the following events are performed for each image:

1. Download the signature of the image
2. Download the image file
3. Perform CRC check
4. Install the image

Even if it encounters a failure in one of the images, it will proceed to upgrade the other images.

In systems running MR2 management modules

In systems running MR2 management modules, all images and their signature files are first downloaded and saved to temporary files in the embedded Slot1 Compact Flash. Once all the images are successfully downloaded, the system proceeds to install them.

> NOTE
> If there is any failure during download operation for any file copy, the entire operation is terminated and a messages is posted to the syslog. For a list of Simplified Upgrade syslog messages, refer to Syslog messages for Simplified Upgrade and Auto Upgrade on page 58.

The following events occur during the install operation:

- perform a CRC check
- install the image

Version Check

Prior to this release, Simplified Upgrade and LP Auto-Upgrade reads the manifest file for the location of the image to be used for the upgrade, and proceeds to download the image file.

For instance, when Simplified Upgrade is upgrading the LP FPGA of the interface modules, it downloads the bundled FPGA file then later attempt to install individual FPGA types to the applicable interface modules. In the individual FPGA installation, it performs a version check between the downloaded image and the currently running image.

If both versions are the same, Simplified Upgrade will skip the upgrade for that FPGA type and proceed to the next FPGA type. In a case where all interface modules are up-to-date, all will be skipped.

Version Information

This release will address the above mentioned example by introducing version checking at the beginning. The manifest file will now have a version field for every specified image. For example, a line in a manifest file for XPP MRJ FPGA image may look something like this,

```
xppmrj_05600.bin 1.00
xpp8x10_05600i066.bin 6.14
pbif8x10_05600i066.bin 1.30
```

For every FPGA type in the manifest file that is applicable to the system, its version will be compared to the image that is currently running. If any of the following conditions is satisfied, it will start to download the bundled FPGA image and proceed to install the applicable FPGAs conditionally:

- At least one card is not in UP state.
- At least one FPGA type version does not match.
- Failure to retrieve the running version (due to internal error).

Otherwise, if all the FPGA types match the versions, Simplified Upgrade will skip this step. The display output will look like this:

```
Bundled FPGA skipped, same version exists.
```

Option to Ignore the Version

By default, the upgrade operation will perform a version check. An optional parameter to ignore the version field will be available in the CLI command as well as SNMP MIB.

The user may choose to perform a forced upgrade.

Similarly, if the specified manifest file does not have a version field, it will perform a forced upgrade for backward compatibility.

Supported Images

The version comparison is done for the following images:

- Interface Module FPGA (LP FPGA)
- Management Module FPGA (MBRIDGE and MBRIDGE-32)

NOTE
Simplified Upgrade (single-command) must be performed before LP Auto-Upgrade can be configured. The later one uses the manifest file that the former one downloaded in the system flash.

Summary Report

During the simplified upgrade process, the system keeps track of the status of every image download, validation and installation and creates a summary report that is displayed at the end of the upgrade. If any image download or installation fails, the summary report indicates the operation failed and details of the failure. You can individually upgrade any failed images using existing upgrade commands for individual images. The summary report also identifies any potential incompatibility issues.

The summary report display is modified to indicate that the upgrade was skipped for the image. It will appear similarly to the example report as follows:

```
System Upgrade Done.
Upgrade Summary
Source: tftp 10.120.75.21 Directory /XMR-MLX
1) Installed /XMR-MLX/Boot/ManagementModule/xmprm05600.bin to MP Boot
2) Installed /XMR-MLX/Boot/InterfaceModule/xmlprm05600.bin to LP Boot on all LP slots
3) Installed /XMR-MLX/Monitor/ManagementModule/xmb05600.bin to MP Monitor
4) Installed /XMR-MLX/Monitor/InterfaceModule/xmlb05600.bin to LP Monitor on all LP slots
5) Installed /XMR-MLX/Application/ManagementModule/xmr05600b296.bin to MP Primary
6) Installed /XMR-MLX/Application/InterfaceModule/xmlp05600b296.bin to LP Primary on all LP slots
7) Skipped LP FPGA Bundled, same version exists.
8) Installed /XMR-MLX/FPGA/ManagementModule/mbridge_05600b296.xsvf to FPGA MBRIDGE
Checking for coherence...
Done.
```

Single-Command Package Upgrade

The CLI command is modified to have an optional parameter to ignore or bypass version checking.

Full syntax (using a TFTP server as the source):

```
device# copy tftp system [all-images] <server-ip-address>
manifest <File name> [lp-sec | mp-sec | secondary]
[skip-version-check]
```

Full syntax (using a removable storage device as the source):

```
device# copy <slot1 | slot2> system [all-images]
manifest <File name> [lp-sec | mp-sec | secondary]
[skip-version-check]
```

Interface Module Auto-Upgrade

> NOTE
> Interface Module Auto-Upgrade does not support LP Auto-Upgrade, which allows the system to automatically upgrade the Boot and FPGA images of an inserted interface module.

In a full-system upgrade where an external set of images (or, release package) is to be applied to the system, it makes sense to perform a version comparison between what is currently running in the system and the release package (while LP Auto-Upgrade compares the image version in LP and that of the system).

Upgrading the software

The command can be issued to specify the source of the images, whether it is from a TFTP server or auxiliary storage device.

Upgrading the software using a TFTP server

To upgrade the management and interface boot, monitor, and application images, as well as FPGA images, enter the following command using TFTP as the source of the images.

The full syntax for the command when using a TFTP server is as follows:

```
device# copy tftp system [all-images]<server-ip-address> manifest
 <File name> [lp-sec | mp-sec| secondary
```

The following parameters are available:

- The optional parameter [**all-images**] specifies that the management and interface boot, monitor, and application images, as well as FPGA images should be upgraded. If the parameter is not entered, only the management and interface monitor and application images and bundled FPGA image for interface modules which don't include MBRIDGE and SBRIDGE are upgraded.
- The parameter *server-ip-address* pecifies the TFTP server IP address in IPv4 or IPv6.
- The parameter *File name* specifies the manifest filename, including its relative path to the TFTP server root directory.
- The optional parameter [**lp-sec** | **mp-sec** | **secondary**] specifies the destination code image. If not specified, it defaults to primary for both MP and LP. This is for the application image only.
  - **lp-sec** specifies that MP image goes to primary while LP goes to secondary.
  - **mp-sec** specifies that MP image goes to secondary while LP image goes to primary.
  - **secondary** means both MP and LP images goes to secondary.

Upgrading the software using an auxiliary storage device

The storage card must have the manifest file at the top-most of the base directory and all the images must be in the directory structure specified in the manifest file.

The full syntax for the command when using an auxiliary storage device is as follows:

```
device# copy
 <slot1|slot2> system [all-images] manifest
 <filename
>
[lp-sec | mp-sec | secondary]
```

The following parameters are available:

- The parameter *slot1* | *slot2* identifies the source auxiliary storage device slot number.
- The optional parameter [**all-images**] specifies that the management and interface boot, monitor, and application images, as well as FPGA images, including MBRIDGE and SBRIDGE, should be upgraded. If the parameter is not entered, only the management and interface monitor and application images and bundled FPGA image for interface modules which don't include MBRIDGE and SBRIDGE are upgraded.
- The parameter *filename* specifies the manifest filename, which should be located at the root directory of the storage device.
- The optional parameter [**lp-sec** | **mp-sec** | **secondary**] specifies the destination code image. If not specified, it defaults to primary for both MP and LP. This is for the application image only.
  - **lp-sec** specifies that MP image goes to primary while LP goes to secondary.
  - **mp-sec** specifies that MP image goes to secondary while LP image goes to primary.
  - **secondary** means both MP and LP images goes to secondary.

Auto upgrade

NOTE
This feature is available only on devices that have been upgraded to R05.3.00 or later using the Simplified Upgrade feature as it requires the manifest file.

NOTE
The auto upgrade feature is disabled by default and must be enabled to take effect.

If you have used the simplified upgrade procedure to upgrade your system to R05.3.00 or later, you can take advantage of the auto upgrade feature. The auto upgrade feature allows the system to automatically upgrade the images of a newly inserted interface module if it detects a mismatch in monitor and application image files, as synched in releases prior to R05.3.00 or later, as well as boot and FPGA image files, depending on the parameters used.

In systems running MR management modules

If the device is running an MR management module, it will take the following steps:

1. Perform a signature check of the manifest file.
2. Open the manifest file to lookup for the filename of the image and its relative path.
3. For the TFTP source, download the image using the TFTP info specified in **lp auto-upgrade tftp** command. For the case of storage card source, it will copy the image from the specified auxiliary storage slot number.
4. Install the image to the destination interface module.

It will repeat the same steps for all images necessary for the upgrade.

If an image cannot be located, an error is logged and it will proceed to boot with application and monitor images synced from the MP.

In systems running MR2 management modules

For devices running an MR2 management module, the images lp-boot and lp-fpga-all, kept in the flash memory, are used. If the image is not found in the flash memory, the system downloads it from the source specified in the command (TFTP or storage card).

At the end of the auto-upgrade process, regardless if it was completed successfully or not, syslog messages and traps are posted.

Enabling Auto Upgrade

NOTE
The auto upgrade feature is disabled by default and must be manually enabled to take effect.

The full syntax for the command is as follows:

```
device(config)# lp auto-upgrade <slot1 | slot2 | tftp <ip-address
>> [path <directory pathname>]
```

Parameter descriptions:

- The parameter **tftp***server-ip-address* specifies the TFTP server IP address in IPv4 or IPv6.
- The parameter **slot1** | **slot2** specifies the source auxiliary storage device slot number.
- The optional parameter [path *directory pathname*] specifies the relative path of the manifest file in the TFTP server directory file structure. This should not include the manifest file name. If not specified, it defaults to the TFTP root.

NOTE
The path specified, plus the build directory and file names of the various files should not exceed 127 characters.

To enable the auto upgrade feature of interface modules in your device from a TFTP, enter the following:

```
device(config)# lp auto-upgrade tftp <ip-address> [path <directory pathname
>]
```

To enable the auto upgrade feature of interface modules in your device using a auxiliary storage device, enter the following:

```
device(config)# lp auto-upgrade <slot1 | slot2> [path <directory pathname
>]
```

At the end of the auto-upgrade process, regardless if it was completed successfully or not, syslog messages and trap are posted.

Disabling Auto Upgrade

NOTE
The auto upgrade feature is disabled by default and must be manually enabled to take effect.

Auto-upgrade of interface module can be disabled by applying 'no' to the command. When the auto upgrade feature is disabled, the newly inserted interface modules boot after syncing the application and monitor images from the management module without syncing the interface boot image and interface FPGAs.

To disable the auto upgrade feature of interface modules in your device, enter the following:

```
device(config)# no lp auto-upgrade
```

This will post a syslog after the completion of the process, whether successful or not.

Syslog messages for Simplified Upgrade and Auto Upgrade

Table 4 lists the syslog messages related to the simplified upgrade procedure and auto upgrade feature.

TABLE 4 Simplified Upgrade and Auto Upgrade syslog messages

Event Description	Message
Simplified upgrade has started	`Single-command upgrade has started.`

Simplified upgrade is complete	`Single-command upgrade completed.`
	or
	`Single-command upgraded with error(s).`

Auto upgrade has started	`Auto-upgrade for slot <slot-id> has started.`

Auto upgrade is complete	`Auto-upgrade for slot <slot-id> completed.`
	or
	`Auto-upgrade for slot <slot-id> completed with errors.`

The following SNMP traps are generated:

snTrapUpgradeSingleCmdStart ::= { snTraps 1216 }

snTrapUpgradeSingleCmdDone ::= { snTraps 1217 }

snTrapAutoUpgradeStart ::= { snTraps 1218 }

snTrapAutoUpgradeDone ::= { snTraps 1219 }

For more information on the SNMP traps, refer to the *Unified MIB Reference* .

MIB information for Simplified Upgrade and Auto Upgrade

For MIB information related to the simplified upgrade and auto upgrade features, refer to the *Unified IP MIB Reference* document.

SCP based simplified upgrade

A Python script is available that copies files to the device (MLXe) compact flash using the SCP server functionality on the device from a remote SCP client, and then issues a Simplified Upgrade from compact flash. This script runs on a remote Linux platform.

> NOTE
> Only MLXe devices with MR2 management cards are supported.

The following use case examples provide the process to perform the following:

- Copy files to compact flash and do a simplified upgrade
- Copy files to compact flash
- Verify the copied files

Use case: Copy files to compact flash and do a simplified upgrade

The following example copies files to compact flash /slot1 and performs a simplified upgrade.

NOTE

Login password can be provided on the command line or interactively (with masking).

```
# python sbsupgrd.py --device xx.yy.zz.1 \
         --manifest 06100p296/XMR-MLX/MLX06100p296_mnf.txt \
         --subdir 06100p296 -cf slot1 \
         --user xyz [--passwd xyz_pass]
…
2016-06-06 20:47:12,538 - __main__ - INFO - Stage: Argument Parser: Started
2016-06-06 20:47:12,538 - __main__ - INFO - Arguments: -v 0, --device xx.yy.zz.1, --manifest 06100p296/XMR-
MLX/MLX06100p296_mnf.txt, --cf slot1, --subdir 06100p296,  --user lab, --passwd ***
Password:
2016-06-06 20:47:12,540 - __main__ - INFO - Stage: Manifest Parser: Started
2016-06-06 20:47:12,540 - __main__ - INFO - Stage: Manifest Parser: Opening 06100p296/XMR-MLX/
MLX06100p296_mnft.txt
2016-06-06 20:47:12,564 - __main__ - INFO - Stage: Manifest Parser: Closed 06100p296/XMR-MLX/
MLX06100p296_mnf.txt
2016-06-06 20:47:12,570 - __main__ - INFO - Stage: Copier: Started
2016-06-06 21:08:52,722 - __main__ - INFO - Stage: SignatureValidator: Started
2016-06-06 21:15:33,346 - __main__ - INFO - Stage: Installer: Started
…
System Upgrade Done.
Upgrade Summary
  Source: storage card slot1 Directory 06100p296/XMR-MLX
1) Installed /XMR-MLX/Boot/ManagementModule/xmprm06100.bin to MP Boot
2) Installed /XMR-MLX/Boot/InterfaceModule/xmlprm06100.bin to LP Boot on all LP slots
3) Installed /XMR-MLX/Monitor/ManagementModule/xmb06100.bin to MP Monitor
4) Installed /XMR-MLX/Monitor/InterfaceModule/xmlb06100.bin to LP Monitor on all LP
slots
5) Installed /XMR-MLX/Application/ManagementModule/xmr06100b296.bin to MP Primary
6) Installed /XMR-MLX/Application/InterfaceModule/xmlp06100b296.bin to LP Primary on
all LP slots
7) Skipped LP FPGA Bundled, same version exists.
8) Installed /XMR-MLX/FPGA/ManagementModule/mbridge_06100b296.xsvf to FPGA MBRIDGE
Checking for coherence...
Done
```

Use case: Copy files to compact flash

The following example copies files to compact flash.

```
# python sbsupgrd.py --device xx.yy.zz.1 \
         --manifest 06100p296/XMR-MLX/MLX06100p296_mnf.txt \
         --subdir 06100p296 -cf slot1 --stage Copier \
         --user xyz
```

Use case: Verify the copied files

The following example verifies the files that were copied files to compact flash.

```
# python sbsupgrd.py --device xx.yy.zz.1 \
         --manifest 06100p296/XMR-MLX/MLX06100p296_mnf.txt \
         --subdir 06100p296 -cf slot1 --stage SignatureValidator \
         --user xyz
```

In addition to the signature based verification above, you can also perform a separate signature based firmware integrity check when the image is installed on the device in step, if the **enable firmware-integrity-check** command is enabled.

Loading and saving configuration files

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

Extreme MLX Series and 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** command 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:

```
device(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:

```
device(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.

```
device# 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.

```
device# 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 HTTP(S), SCP or TFTP server

To copy the startup-config or running-config file to or from an HTTP(S), 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. For the HTTP(S) server, you can copy to and from to any filename.

Using HTTP(S)

By default, file copies can be done using the management IP. You must configure the source-interface for the HTTP[S] client for file transfers to take place through the interface for a physical, loopback or logical port. Once you configure the LP port as the source interface, transfers will take place using only the configured interface. Connections to the management IP will not be rejected for file copies.

To copy the *startup-configuration* file to an HTTP server, enter the following command:

copy flash http *ip-address filename_server startup-config*

NOTE
filename_server is the name of the file on the server to which the *startup-configuration* file is copied.

To download the *running-config* file to the device from an HTTP server, enter the following command:

copy http slot2 *ip-address running-config filename_device*

To make the *filename_device* the startup configuration file, enter the following command.

copy slot2 startup-config *filename_device*

NOTE
You must use *flash* while performing file copies on CES and CER devices. Using *slot1* or *slot2* is not supported for these devices.

NOTE
Use similar steps for an HTTPS server.

1. HTTPS client uses TLS protocol.
2. In FIPS mode HTTP client protocol will be hidden (HTTPS is still shown).
3. TLS 1.0, TLS 1.1,and TLS 1.2 versions are supported.
4. SSL 3.0 is not supported.

NOTE

1. You can perform only one HTTP(S) file transfer at a time. Parallel transfers will be blocked across HTTP/HTTPS/SCP/TFTP with the following error message: "Error: HTTP[S]: Another TFTP/SCP/HTTP[S] copy operation is in progress. Please try later".
2. When using HTTP, base64-encoded username and password may be seen by a network packet capture tool.
3. File size is limited to 200 Mbyte, provided there is space in the FLASH memory of the target destination for the transfer to the device.
4. Certain filenames such as *startup-config* and *running-config* are reserved. The system will warn you and generate an error message when you try to use any reserved filename, which is an ineligible target for the copy command.

   NOTE
   If you copy an invalid image to the FLASH and make it the primary image, a reload may fail to bring up the device.

5. HTTP(S) client file transfer is supported for the default VRF only.

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

Secure copy (SCP) supports file transfer between local and a remote hosts. It combines the file-transfer element of BSD remote copy (RCP) with the authentication and encryption provided by the Secure shell (SSH) protocol.

The SCP client feature on Extreme NetIron devices helps to transfer files to and from the SCP server and maintains the confidentiality of the data being transferred by blocking packet sniffers from extracting valuable information from the data packets. You can use SCP client to do the following:

- Download a boot file, NetIron application image file, signature file, license file, startup configuration file, or running configuration from an SCP server
- Upload a NetIron application image file, startup configuration file, or running configuration to an SCP server

SCP client uploads the file to the SCP server (that is, the SSH server) by providing files to be uploaded. You can specify file attributes, such as permissions and time-stamps as part of file data when you use SCP client to upload files. SCP client supports the same copy features as the time stamps, TFTP client feature on NetIron devices, but the SSH2 protocol secures data transfer.

Uploading an image to an SCP server

To securely upload image files to a secure copy (SCP) server, copy an image from a device to the SCP server.

```
device# copy flash scp 10.20.99.146 ~/xmr05800.bin primary
```

Uploading configuration files to an SCP server

To securely upload startup and running configuration files to a secure copy (SCP) server.

1. Copy a startup configuration file to the SCP server.

   ```
   Device#copy startup-config  scp 10.20.1.1 icx-74-startup
   ```

   The startup configuration file is uploaded to the SCP server and you are notified when the transfer is complete.

   ```
   device#copy startup-config scp 172.20.133.116 run.txt
   User name:tester
   Password:
   Connecting to remote host......
   Connection Established. Uploading .Done.
   startup-config upload via SCP complete.

   Connection Closed
   device#
   ```

2. Copy a running configuration file to the SCP server.

   ```
   Device#copy running-config  scp 10.20.1.1 icx-74-run
   ```

Downloading configuration files from an SCP server

To securely download startup and running configuration files from a secure copy (SCP) server to a device.

1. Copy a startup configuration file from the SCP server.

```
device# copy scp startup-config 10.20.1.1 icx-74-startup
```

2. Copy a running configuration file from the SCP server.

```
device# copy scp running-config 10.20.1.1 icx-74-run
```

Making local copies of the startupconfiguration 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:

```
device# 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:

```
device# 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.

Verifying firmware and digital signatures after an SCP download

Use the commands in this section to perform a final checksum after an SCP download of firmware.

To ensure that downloaded code is an exact duplicate of the original, the following commands.

This command enables the RSA2048 key and SHA256 hash digital signature based firmware integrity check when the image is downloaded and installed on the device, or when the device is rebooted.

```
device(config)# enable firmware-integrity-check
```

Using SHA256 checksum commands

The syntax of the **verify** command is discussed in the following examples.

Syntax: verify md5 | sha1 | sha256 file *filenm*| **digest-file** *filenm*

To print and verify the SHA256 digest of the startup-config file the following command can be used.

```
device# verify sha256 file startup-config
```

To verify the SHA256 digest of the startup-config file when the digest is stored in a file, the following command can be used. Similar commands can be used for MD5, and SHA1.

```
device# verify sha256 file startup-config digest-file startup-config.sha256dgst
```

Using the verify signature command

The syntax of the **verify signature file primary signature-file** command is discussed in the following example.

Syntax: verify signature file primary signature-file *filenm*

To verify the signature file of the primary, use the following command.

```
device# verify signature file primary signature-file primary.sig
```

Firmware integrity check commands

The syntax of the command is discussed in the following example.

Syntax: enable firmware-integrity-check

To enable signature based firmware verification of images, use the following command.

```
device(sw)# config terminal
device(config)# enable firmware-integrity-check
```

The following is an example of performing a firmware integrity check when using SCP.

```
device(sw)# config terminal
device(config)# enable firmware-integrity-check

lab@device{286}: scp xmr06100.sha256 lab@10.xx.xx.xx:flash:primary.sig
xmr06100.sha256                       100%  256     0.3KB/s   00:00
Connection to 10.xx.xx.xx closed by remote host.
lab@device{287}: scp xmr06100.bin lab@10.xx.xx.xx:flash:primary
xmr06100.bin                          100%   10MB   2.0MB/s   00:05
Connection to 10.xx.xx.xx closed by remote host.
```

The following is an example of performing a firmware integrity check when using TFTP.

```
device(sw)# config terminal
device(config)# enable firmware-integrity-check

# copy tftp flash 10.xx.xx.xx ce06100.sha256 primary.sig
. TFTP: Download to primary flash done.
# copy tftp flash 10.xx.xx.xx ce06100.bin primary
.....................................................
.....................................................
.............. TFTP: Download to primary flash done.
#
```

The following is an example of performing a firmware integrity check when using PCMCIA.

```
device(sw)# config terminal
device(config)# enable firmware-integrity-check

#copy slot1 flash xmr06100.sha256 primary.sig
#copy slot1 flash xmr06100.bin primary
.....................................................
.....................................................
................................Verified OK
Done
Copy MP PRIMARY IMAGE to standby MP, please wait.
MP images Sync Not Needed.
```

Performing a boot time firmware integrity check

When the image signature is valid, following will be seen in boot time console messages.

```
…
Running FIPS Software/Firmware Integrity Test
Verifying MP Image file primary.....Verified OK
PASSED
Verifying MP Monitor.....Verified OK
PASSED
FIPS Software/Firmware Integrity Test PASSED
```

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 CER 2000 Series and CES 2000 Series 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** command 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:

```
device(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
> Extreme strongly recommends 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:

```
device(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 withthe 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.

```
device# 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.

```
device# 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 HTTP(S), SCP or TFTP server

To copy the startup-config or running-config file to or from an HTTP(S), 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. For the HTTP(S) server, you can copy to and from to any filename.

Using HTTP(S)

By default, file copies can be done using the management IP. You must configure the source-interface for the HTTP[S] client for file transfers to take place through the interface for a physical, loopback or logical port. Once you configure the LP port as the source interface, transfers will take place using only the configured interface. Connections to the management IP will not be rejected for file copies.

To copy the *startup-configuration* file to an HTTP server, enter the following command:

copy flash http *ip-address filename_server startup-config*

> NOTE
> *filename_server* is the name of the file on the server to which the *startup-configuration* file is copied.

To download the *running-config* file to the device from an HTTP server, enter the following command:

copy http slot2 *ip-address running-config filename_device*

To make the *filename_device* the startup configuration file, enter the following command.

copy slot2 startup-config *filename_device*

NOTE
You must use *flash* while performing file copies on CES and CER devices. Using *slot1* or *slot2* is not supported for these devices.

NOTE
Use similar steps for an HTTPS server.

1. HTTPS client uses TLS protocol.
2. In FIPS mode HTTP client protocol will be hidden (HTTPS is still shown).
3. TLS 1.0, TLS 1.1,and TLS 1.2 versions are supported.
4. SSL 3.0 is not supported.

NOTE

1. You can perform only one HTTP(S) file transfer at a time. Parallel transfers will be blocked across HTTP/HTTPS/SCP/TFTP with the following error message: "Error: HTTP[S]: Another TFTP/SCP/HTTP[S] copy operation is in progress. Please try later".
2. When using HTTP, base64-encoded username and password may be seen by a network packet capture tool.
3. File size is limited to 200 Mbyte, provided there is space in the FLASH memory of the target destination for the transfer to the device.
4. Certain filenames such as *startup-config* and *running-config* are reserved. The system will warn you and generate an error message when you try to use any reserved filename, which is an ineligible target for the copy command.

   NOTE
   If you copy an invalid image to the FLASH and make it the primary image, a reload may fail to bring up the device.

5. HTTP(S) client file transfer is supported for the default VRF only.

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 startupconfiguration 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:

```
device# 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 Extreme NetIron 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 8 or more ports, you must change the ifindex. Refer to ifIndex allocation on page 22.
- Before you install your 100xGbE 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.

```
device(config)# system-init fabric-data-mode force-normal
device(config)# system-init tm-credit-size credit_1024b
device(config)# exit
device# write memory
device# reload
```

For more information about how to install 100xGbE modules, refer to the appropriate 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)

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 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.

> NOTE
> Do not attempt to downgrade NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules or high-speed switch fabric modules to software versions older than R05.0.00c. The modules will not operate with older software.

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 MLX Series and XMR Series 16-slot devices, you must also install high-speed fans. Refer to the 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.

Management module considerations

Upgrading to MR2 management modules

This section describes how to upgrade the management module in your router to an MR2 management module.

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. If the MR2 router no longer boots, please contact Extreme technical support.

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

1. Perform a basic upgrade of your devices to NetIron Release 5.2.00b as documented in the appropriate chapter in this document 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:

   ```
   device
   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 userdevice-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 dst-file:startConfig
   ```

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 the hardware installation guide 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
```

   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-addressfilename*

     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

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**

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

Setting port auto-negotiation

Perform the port auto-negotiation procedure after upgrading to R06.0.00 and later releases.

Perform this task when upgrading to R6.0.00 and later releases with 20x10GE or 4x10GE IPSEC modules installed.

When a device is upgraded to R06.0.00 and later releases from R5.7.00x, R5.8.00x, or R05.9.00x where auto-negotiation is supported, the auto-negotiation feature will be disabled for the interfaces of existing 20x10GE and 4x10GE-IPSEC modules. The following task will enable auto-negotiation.

1. Use the **interface eth** command to direct the specific interface.
2. Execute the **gig-default auto-gig** command to enable auto-negotiation on the interface.

```
device(config)#interface eth 8/1
device(config-if-e10000-8/1)#gig-default auto-gig
device(config-if-e10000-8/1)#
```

Troubleshooting

This appendix contains information about specific scenarios and troubleshooting issues that you may find useful when you perform your Extreme NetIron 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.

```
device(config)# cluster abc 1
device(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.

```
device(config-cluster-abc)# no client-interfaces shutdown
```

NOTE

This process must be done for 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>
```

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 and later, 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 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 1G modules stuck in down state

The use of the "wait-for-all-cards" configuration in NetIron Release 5.3.00 may cause ports on any 1G module to stay down after boot-up, even if configured to be enabled.

To avoid such an occurrence, it is recommended that the "wait-for-all-cards" configuration be removed from the startup-config prior to reloading the router with R05.3.00 code.

To bring the port back from a "down" state, disable and re-enable the port.