

Extreme SLX-OS Software Upgrade Guide, 18r.2.00

Supporting the ExtremeRouting SLX 9850 and SLX 9640 and the
ExtremeSwitching SLX 9540 Devices

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.....	5
Conventions.....	5
Notes, cautions, and warnings.....	5
Text formatting conventions.....	5
Command syntax conventions.....	6
Documentation and Training.....	6
Training.....	6
Getting Help.....	6
Subscribing to Service Notifications.....	7
Providing Feedback to Us.....	7
About This Document.....	9
What's new in this document	9
Supported hardware.....	9
Interface module capabilities.....	10
Software Installation.....	11
Prepare for the installation.....	11
Installation procedure.....	12
Installing and Maintaining Firmware.....	15
Firmware management overview.....	15
Preserving the configuration.....	15
Automatic firmware synchronization.....	15
Connecting to the device.....	16
Upgrading considerations and restrictions.....	16
Prerequisites for firmware download.....	16
Obtaining the firmware version.....	17
Obtaining and decompressing firmware.....	17
Standard method for downloading firmware.....	18
Downloading firmware using the default-config option.....	19
Downloading firmware using the coldboot option.....	20
Downloading firmware from a USB device.....	21
Upgrading to 64-bit systems.....	22
Peripheral firmware upgrades.....	22
SLX 9850 fpga upgrade.....	23
SLX 9540 fpga upgrade.....	26
SLX 9540 CPLD image upgrade.....	27
Upgrading devices with BGP neighbor send-community configuration.....	27
Downgrading considerations and restrictions.....	28
SLX-OS Capabilities.....	31
Viewing software capabilities.....	31

Preface

- Conventions..... 5
- Documentation and Training..... 6
- Getting Help..... 6
- Providing Feedback to Us..... 7

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.
<i>italic text</i>	Identifies text to enter in the GUI. 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.
<i>italic text</i>	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, <i>member[member...]</i> .
\	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

- [What's new in this document](#) 9
- [Supported hardware](#)..... 9

What's new in this document

This document is released with Extreme SLX OS 18r.2.00.

The SLX-OS 18r.2.00 release is the first SLX-OS release that supports SLX 9640 devices.

TABLE 1 Summary of enhancements in this SLX-OS release

Feature	Description	Described in
SLX 9640 support	Software installation preparation and procedure.	Software Installation on page 11
BGP large communities	Considerations for upgrading and downgrading devices with BGP neighbor send-community configurations.	Upgrading devices with BGP neighbor send-community configuration on page 27

TABLE 2 Additional changes

Feature	Description	Described in
Firmware download CLI through USB	Added note on decompressing firmware in the Obtaining and decompressing firmware section. Added note on downloading firmware through USB3.0 in the Downloading firmware from a USB device section. Added note on USB-based firmware upgrade from SLX-OS 17r.1.01b in the Upgrading to 64-bit systems section.	Installing and Maintaining Firmware

For complete release information, refer to the SLX OS Release Notes.

Supported hardware

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

Although many different software and hardware configurations are tested and supported by this release, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- ExtremeRouting SLX 9850-4 router
- ExtremeRouting SLX 9850-8 router
- ExtremeRouting SLX 9640 router
- ExtremeSwitching SLX 9540 switch

To obtain information about other releases, refer to the documentation specific to that release.

Interface module capabilities

The following table lists the supported capabilities for the following SLX 9850 interface modules:

- BR-SLX9850-10Gx72S-M
- BR-SLX9850-100Gx36CQ-M
- BR-SLX9850-10Gx72S-D
- BR-SLX9850-100Gx36CQ-D
- BR-SLX9850-100Gx12CQ-M

TABLE 3 SLX 9850 interface modules capabilities

Capability	Modular interface module
MPLS	Yes
Packet buffer memory per interface module	12GB (BR-SLX9850-10Gx72S-M) 36GB (BR-SLX9850-100Gx36CQ-M) 8GB (BR-SLX9850-10Gx72S-D) 24GB (BR-SLX9850-100Gx36CQ-D) 8GB (BR-SLX9850-100Gx12CQ-M)

Software Installation

- Prepare for the installation.....11
- Installation procedure..... 12

Prepare for the installation

To prepare for the installation, perform the following tasks.

NOTE

In the unlikely event of a failure or timeout, you will be able to provide your router support provider the information required to troubleshoot the problem by performing the tasks.

1. Ensure that all production traffic is detoured from the device that is under-going the firmware upgrade.
2. Ensure that network connectivity is established to allow the **scp** or **ftp** command to complete the FWD download of the image to the devices. For example, enter the following command to verify network connectivity:

```
# ping <server_address>
```

3. Prepare to complete the firmware upgrade steps using a console with access to the device.
4. Save the "startup-config" file to a remote server. For example, enter the following command to save the file:

```
# copy running-config tftp://@<server_address>/
```

5. Complete the pre-requisites for the installation by collecting the system context using the following commands:

- **show version**
- **show chassis**
- **show environment fan/power/history/sensor/temp**
- **show interface status**
- **show license**
- **show firmwaredownloadhistory**
- **show firmwaredownloadstatus**
- **show media**
- **show run**

6. Enter the following FTP firmware download command:

```
# firmware download ftp coldboot user <username> password <password> file release.plist directory <file_path> host <server_ip>
```

7. Enter the following USB firmware download command, where "SLX-OS_vX.X.X" refers to the current version number:

```
# firmware download usb coldboot directory SLX-OS_vX.X.X
```

8. Verify the system after the firmware download. For example, enter the following commands to verify the firmware was downloaded:

- **show version**
- **show firmwaredownloadstatus**
- **show firmwaredownloadhistory**

Installation procedure

To complete the installation, perform the following tasks.

1. Login to the SLX device.
2. Check the license to make sure that the `ADVANCED_FEATURES` license exists by entering the following command:

```
device# show license
```

3. Login to the SLX device as root.
4. Change directories to the `/tftpboot` directory by entering the following command:

```
[root@SLX]# cd /tftpboot
```

5. Find the folder named `SWBD2900`. Check that the `SWBD2900` folder is empty by entering the following command:

```
[root@SLX]# ls -las SWBD2900/*.*
```

6. Copy the TPVM package from image folder (Location = `/dist/SWBD2900`) to the device by entering the following command:

```
[root@SLX]# scp /dist/SWBD2900/*. * SWBD2900/.
```

7. Check the contents of the directory `/tftpboot/SWBD2900` to make sure that the file is copied correctly. For example:

```
[root@SLX]# ls -las SWBD2900/*.*
```

8. Change directory to the `/fabos/users/admin` directory and install the TPVM package using the `tpvmadm install` command. For example:

```
[root@SLX]# cd /fabos/users/admin
[root@SLX]# pwd
/fabos/users/admin
[root@SLX]# tpvmadm install
Installation starts. To check the status use 'show' command
```

9. Enter the `tpvmadm show` command to check the status of the installation. For example:

```
[root@SLX]# tpvmadm show
TPVM is being installed now
[root@SLX]#
```

10. Start TPVM and check the status. For example:

```
[root@SLX]# tpvmadm show
TPVM is installed but not running, and AutoStart is disabled on this host.
[root@SLX]# tpvmadm start
start succeeds
[root@SLX]# tpvmadm show
TPVM is running, and AutoStart is disabled on this host.
[root@SLX]#
timed out waiting for input: auto-logout
```

11. Enable auto-boot and reload the system. This can be done either from the root or SLX device prompt. For example:

```
[root@SLX]# tpvmadm enable_on_boot
enable_on_boot succeeds
[root@SLX]#
```

or:

```
device# tpvm auto-boot enable
auto-boot enable succeeds
device# reload system
```

12. Verify the TPVM status after the device reload. For example:

```
[root@SLX]# tpmadm show
TPVM is running, and AutoStart is enabled on this host.
[root@SLX]#
```

NOTE

In the unlikely event of a failure or timeout, provide your router support provider the information prepared per the instructions in the Prepare for the installation section to troubleshoot the problem.

Installing and Maintaining Firmware

• Firmware management overview.....	15
• Automatic firmware synchronization.....	15
• Connecting to the device.....	16
• Upgrading considerations and restrictions.....	16
• Prerequisites for firmware download.....	16
• Obtaining the firmware version.....	17
• Obtaining and decompressing firmware.....	17
• Peripheral firmware upgrades.....	22
• Upgrading devices with BGP neighbor send-community configuration.....	27
• Downgrading considerations and restrictions.....	28

Firmware management overview

Extreme firmware upgrades consist of multiple firmware packages listed in a .plist file. The .plist file contains specific firmware information (time stamp, platform code, version, and so on) and the names of the firmware packages to be downloaded. These packages are made available periodically to add features or to remedy defects in the firmware. In SLX-OS, the firmware upgrade is performed incrementally. The **firmware download** command compares the new firmware packages against the current installation and only downloads the packages that contain new features or have been modified.

You can download the firmware from a remote server by means of the File Transfer Protocol (FTP), SSH File Transfer Protocol (SFTP), Trivial File Transfer Protocol (TFTP), or Secure Copy Protocol (SCP). If you want to download firmware from a remote server, you must connect the management Ethernet port of the router to the server. In a modular chassis, both management Ethernet ports must be connected. Downloading from an Extreme proprietary USB drive is also supported.

If a firmware download session is interrupted by an unexpected reboot, SLX-OS attempts to recover the previously installed firmware. Success depends on the state of the firmware download. You must wait for the recovery to complete before initiating another firmware download.

Preserving the configuration

To preserve the configurations, back up the configuration using the **copy running-config filename** command before the firmware download. After the upgrade is completed, run the **copy filename running-config** command.

Automatic firmware synchronization

When you replace or insert a second management module into a chassis, the active management module automatically synchronizes the hot-plugged standby management module with the same firmware version. The standby management module restarts with the upgraded firmware. The automatic firmware synchronization takes place only if all of the following conditions are met:

- The standby management module is inserted while the chassis is already up (hot-plugged insert).
- There was no firmware download process running when the standby management module was inserted.
- The active and standby firmware versions must be different.

NOTE

Automatic firmware synchronization is intrinsic to SLX-OS and no corresponding **enable** or **disable** commands are associated with automatic firmware synchronization. As a result, the automatic firmware synchronization cannot be disabled.

Connecting to the device

When you upgrade firmware in default mode, you connect to the device through the management IP address.

Use the **show system** command to display the management IP address for the chassis.

```
device# show system
Stack MAC                : 60:9c:9f:b0:92:00

  -- UNIT 0 --
Unit Name                 : cedar-spine-2
Ethernet Port(s)         : 32
Up Time                   : up 17 days 0:33
Current Time              : 23:20:38 GMT
SLX-OS Version            : 17s.1.0017s.1.00_bld63
Jumbo Capable             : yes
Burned In MAC             : 60:9C:9F:B0:93:1A
Management IP             : 10.20.234.119 <- Chassis Management IP address
Management Port Status    : UP

  -- Power Supplies --
PS1 is faulty
PS2 is OK

  -- Fan Status --
Fan 1 is Ok, speed is 6409 RPM
Fan 2 is Ok, speed is 6225 RPM
Fan 3 is Ok, speed is 6225 RPM
Fan 4 is Ok, speed is 6409 RPM
Fan 5 is Ok, speed is 6409 RPM
Fan 6 is Ok, speed is 6409 RPM
```

NOTE

You must configure the gateway and default route that is pointing to the management interface within the management VRF and address-family unicast context.

Upgrading considerations and restrictions

Consider the following when upgrading your firmware version:

- Upgrading SLX-OS is automatically allowed because the Telnet server and SSH server status are enabled by default.
- Upgrading SLX-OS is a disruptive event and reboots the device.

Prerequisites for firmware download

To prepare for a firmware download, perform the following tasks. In the unlikely event of a failure or timeout, you will be able to provide your router support provider the information required to troubleshoot the firmware download.

1. Verify the current firmware version. Refer to [Obtaining the firmware version](#) on page 17.
2. Download the firmware package from the Extreme website to an FTP server.
3. Decompress the firmware archive. Refer to [Obtaining and decompressing firmware](#) on page 17.

4. Decide on a migration path. Check the connected devices to ensure firmware compatibility. Refer to the "SLX-OS Compatibility" section of the *SLX-OS Release Notes* for the recommended firmware version.
5. In a modular system, if you are to download firmware from a file server, verify that the management ports on both MMs are connected to the firmware file server.
6. Back up your router configuration using the **copy running-config filename** command before the firmware download.
7. For additional support, connect the router to a computer with a serial console cable. Ensure that all serial consoles and any open network connection sessions, such as Telnet, are logged and included with any trouble reports.
8. Enter the **copy support** command to collect all current core files prior to executing the firmware download. This information helps to troubleshoot the firmware download process in the event of a problem. Once the **copy support** command is issued collects the files, you can use the **clear support** command to remove the files from the list.
9. Enter the **clear logging raslog** command to erase all existing messages in addition to internal messages.

Obtaining the firmware version

Enter the **show version** command to obtain the firmware version for both primary and secondary partitions of each module.

```
device# show version

SLX-OS Operating System Software
SLX-OS Operating System Version: 17r.1.00
Copyright (c) 2014-2018 Extreme Networks, Inc.
Firmware name:      17r.1.00_bfd_fix
Build Time:         05:11:01 Aug 20, 2016
Install Time:       18:32:33 Aug 22, 2016
Kernel:             2.6.34.6

Control Processor:  GenuineIntel with 7890 MB of memory

System Uptime:     0days 12hrs 35mins 29secs

Slot  Name      Primary/Secondary Versions                               Status
-----
M1    SLX-OS  17r.1.00slxos_17r.1.x_maint_160819_1858
      17r.1.00slxos_17r.1.x_maint_160819_1858
      ACTIVE*
```

Obtaining and decompressing firmware

Firmware upgrades are available for customers with support service contracts and for partners on the Extreme Networks website at www.extremenetworks.com.

You must download the firmware package to the protocol variant server, such as FTP or SCP, and decompress the package *before* you can use the **firmware download** command to upgrade the firmware on your equipment.

NOTE

Extreme recommends 7zip or WinRAR to decompress the SLX-OS tar file

You may also download the firmware from a USB drive using the **firmware download usb** command.

When you unpack the downloaded firmware, it expands into a directory that is named according to the firmware version. When issued with the path to the directory where the firmware is stored, the **firmware download** command performs an automatic search for the correct package file type associated with the device.

The following **firmware download** command options are available:

- **coldboot**: Downloads the firmware to the system and reboots the device.
- **default-config**: Removes all configuration and is similar to an initial installation and configuration.
- **fullinstall**: Downloads a larger file selection to cover the differences between 32-bit and 64-bit firmware when upgrading or downgrading the device.
- **usb**: Downloads the firmware to the system without activating it, so the device is not automatically rebooted.

Refer to the *Extreme SLX-OS Command Reference* for complete information on all of the available options for the **firmware download** command.

NOTE

To be able to address the FTP or SCP server by its name, ensure that a Domain Name System (DNS) entry is established for the server.

NOTE

SLX-OS does not support the use of special characters (such as &, !, %, or #) in FTP, TFTP, SFTP, or SCP passwords. If your password contains special characters, the download fails.

Standard method for downloading firmware

The **firmware download** command has several options for downloading firmware for your device that help control the process. For complete information on the **firmware download** command options, refer to the *Extreme SLX-OS Command Reference*.

By default, if you enter the **firmware download** command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves a High Availability failover of the active management module and is non-disruptive. In contrast, both the **coldboot** and **default-config** options involve system reboots and are disruptive to traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as the result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

The follow example shows a typical firmware download:

```
device# firmware download ftp directory /slxos/17r.1.00 host 10.31.2.27 user releaseuser password
releaseuser
```

```
Performing system sanity check...
```

```
This command will use the ISSU protocol to upgrade the system. It will cause a WARM reboot and will require
that existing telnet, secure telnet or SSH sessions be restarted.
```

```
Do you want to continue? [y/n]y
```

Once the process completes, log in to the device and enter the **show version** command. Both partitions on the device or on the modules should contain the new firmware.

```
device# show version
SLX-OS Operating System Software
SLX-OS Operating System Version: 17r.1.00
Copyright (c) 1995-2017 Extreme Networks, Inc.
Firmware name:      17r.1.0017r.1.00
Build Time:        21:24:13 Mar  7, 2017
Install Time:      21:46:10 Mar  9, 2017
Kernel:           2.6.34.6
Host Version:      Ubuntu 14.04 LTS
Host Kernel:       Linux 3.14.17
```

```
Control Processor:   QEMU Virtual CPU version 2.0.0
```

```
System Uptime:     16days 23hrs 48mins 7secs
```

Slot	Name	Primary/Secondary Versions	Status
SW/0	SLX-OS	17r.1.0017r.1.00 17r.1.0017r.1.00	ACTIVE*

Downloading firmware using the default-config option

The **firmware download default-config** command allows you to download new firmware onto the router, clean up the configuration, and then force the router to perform a cold reboot.

This option is useful to prevent issues caused by incompatible configurations between the old and the new firmware.



CAUTION

When you use **firmware download default-config**, traffic is disrupted and the configuration is lost. You must save the configuration information before you execute the command and then restore it afterwards.

1. Download the firmware from the source directory with the default-config option.

```
device# firmware download default-config ftp host 10.xx.xx.3 user fvt password pray4green directory
dist
```

```
Performing system sanity check...
```

```
This command will set the configuration to default.
```

```
This command will cause Cold reboot on both psrtitionss at the same time and will require that
existing telnet, secure telnet or SSH sessions be restarted.
```

```
Do you want to continue? [y/n]: y
```

2. Log back into the device.
3. Enter the **firmware commit** command to commit the new firmware. If you entered **y** after the prompt, the device will commit the firmware automatically upon booting up.

```
device# firmware commit
Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
.....
FirmwareCommit completes successfully.
```

4. Enter the **show version** command. Both partitions on the device or on the modules should contain the new firmware.

```
device# show version
SLX-OS Operating System Software
SLX-OS Operating System Version: 17s.1.00
Copyright (c) 1995-2017 Extreme Networks, Inc.
Firmware name:      17s.1.0017s.1.00
Build Time:        21:24:13 Mar  7, 2017
Install Time:      21:46:10 Mar  9, 2017
Kernel:           2.6.34.6
Host Version:     Ubuntu 14.04 LTS
Host Kernel:      Linux 3.14.17

Control Processor:  QEMU Virtual CPU version 2.0.0

System Uptime:     16days 23hrs 48mins 7secs

Slot  Name      Primary/Secondary Versions      Status
-----
SW/0  SLX-OS  17s.1.0017s.1.00
      17s.1.0017s.1.00
      ACTIVE*
```

Downloading firmware using the coldboot option

The **coldboot** option of the **firmware download** command allows you to download new firmware onto a device and forces the device to perform a cold reboot. For complete information on the **firmware download** command options, refer to the *Extreme SLX-OS Command Reference*.

After the firmware completes downloading, the device reboots. This ensures that both partitions reboot with the same firmware, and prevents any firmware compatibility issues that may exist between the old and the new firmware.



CAUTION

When you use **firmware download coldboot**, traffic is disrupted and the configuration is lost. You must save the configuration information before you execute the command and then restore it afterwards.

1. Download the firmware from the source directory with the **coldboot** option.

```
device# firmware download coldboot ftp host 10.xx.xx.3 user fvt password pray4green directory dist

Performing system sanity check...
This command will set the configuration to default.
This command will cause Cold reboot on both psrtitionss at the same time and will require that
existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue? [y/n]: y
```

2. Log back into the device.
3. Enter the **firmware commit** command to commit the new firmware. If you entered **y** after the prompt, the device will commit the firmware automatically upon booting up.

```
device# firmware commit
Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
.....
FirmwareCommit completes successfully.
```

4. Enter the **show version** command. Both partitions on the device or on the modules should contain the new firmware.

```
device# show version
SLX-OS Operating System Software
SLX-OS Operating System Version: 17s.1.00
Copyright (c) 1995-2017 Extreme Networks, Inc.
Firmware name:      17s.1.0017s.1.00
Build Time:         21:24:13 Mar  7, 2017
Install Time:       21:46:10 Mar  9, 2017
Kernel:             2.6.34.6
Host Version:       Ubuntu 14.04 LTS
Host Kernel:        Linux 3.14.17

Control Processor:  QEMU Virtual CPU version 2.0.0

System Uptime:     16days 23hrs 48mins 7secs

Slot  Name      Primary/Secondary Versions      Status
-----
SW/0  SLX-OS  17s.1.0017s.1.00
      17s.1.0017s.1.00
      ACTIVE*
```

Downloading firmware from a USB device

Extreme Network devices support firmware download from a USB device. Before you can access the USB device, you must enable the device and mount it as a file system. The firmware images to be downloaded must be stored in the factory-configured firmware directory. Multiple images can be stored under this directory.

NOTE

USB3.0 used for firmware download can be in VFAT or EXT4 format.

1. Ensure that the USB device is connected to the device.
2. Enter the **usb on** command in privileged EXEC mode.

```
device# usb on
Trying to enable USB device. Please wait...
USB storage enabled
```

3. Enter the **usb dir** command. In this sample output, the "SLX-OS_vX.X.X" refers to the current version number.

```
device# usb dir
firmwarekey\ 0B 2016 Dec 15 15:13
support\ 106MB 2016 Dec 24 05:36
config\ 0B 2016 Dec 15 15:13
firmware\ 380MB 2016 Dec 15 15:13
SLX-OS_vX.X.X\ 379MB 2016 Dec 15 15:31
Available space on usbstorage 74%
```

4. Enter the **firmware download usb** command followed by the relative path to the firmware directory, where the "SLX-OS_vX.X.X" refers to the current version number.

```
device# firmware download usb directory SLX-OS_vX.X.X
```

5. Enter the **usb off** command to unmount the USB storage device for safe removal.

```
device# usb off
Trying to disable USB device. Please wait...
USB storage disabled.
```

Upgrading to 64-bit systems

SLX-OS supports a limited range of 32-bit and 64-bit hardware. This task downloads a larger file selection to cover the differences between 32-bit and 64-bit firmware when upgrading or downgrading the device.

For complete information on the **firmware download** command options, refer to the *Extreme SLX-OS Command Reference*.

NOTE

USB-based firmware upgrade from SLX-OS 17r.1.01b (32-bit) to SLX-OS 17r.2.01 (64-bit) or later is supported with the **fullinstall** option.

1. Download the firmware from the source directory with the **fullinstall** option.

```
device# firmware download fullinstall ftp user releaseuser password releaseuser file release.plist
host 192.168.1.100 directory /release/SLX_17r.2.01 /dist
Performing system sanity check...
```

You are running firmware download on dual MM system with 'fullinstall' option.

This command will preserve startup-config and license across Firmware download but will require manual re-play of configuration once after User verifies if configurations are compatible to the new image. Manual replay of configs could be achieved using 'copy flash://startup-config running-config' command or 'copy <file> running-config' command.

This command will cause a cold/disruptive reboot and will require that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue? [y/n]:

2. Log back into the device. The **fullinstall** option retains the startup configuration file, and upon the automatic reboot of the device, the startup configuration file is reloaded automatically.
3. Enter the **show version** command. Both partitions on the device or on the modules should contain the new firmware.

```
device# show version
SLX-OS Operating System Software
SLX-OS Operating System Version: 17r.2.01
Copyright (c) 1995-2018 Extreme Networks, Inc.
Firmware name:      17r.2.01
Build Time:        21:24:13 Jul  7, 2018
Install Time:      21:46:10 Jul  9, 2018
Kernel:            2.6.34.6
Host Version:      Ubuntu 14.04 LTS
Host Kernel:       Linux 3.14.17

Control Processor:  QEMU Virtual CPU version 2.0.0

System Uptime:     16days 23hrs 48mins 7secs

Slot  Name      Primary/Secondary Versions                Status
-----
SW/0  SLX-OS  17r.2.01
      17r.2.01
                                     ACTIVE*
```

Peripheral firmware upgrades

Some device peripherals can have their firmware upgraded through a Linux shell.

SLX 9850 fpga upgrade

This procedure updates the fpga (Field Programmable Gate Array) flash with the latest image from the installation package.

1. After the device boots, log in to a Linux shell using the **start-shell**.

```
device# start-shell
```

2. Check the FPGA version. If FPGA version is not latest then use following example to upgrade it.

```
# fpga version
```

3. Use the **sysfpga_upgrade help** command to display the upgrade options and execute the **sysfpga_upgrade <option>** command, where the option is selected from the list below.

```
# sysfpga_upgrade help
===== Fusion Sysfpga Upgrading Help Page =====
to upgrade sysfpga on local MM card to the latest image file:
    sysfpga_upgrade mm

to upgrade sysfpga on a remote F4 LC lc1/lc2/lc3/lc4 card to the latest image file:
    sysfpga_upgrade lc1
    sysfpga_upgrade lc2
    sysfpga_upgrade lc3
    sysfpga_upgrade lc4

to upgrade sysfpga on a remote F8 LC lc1/lc2/./lc8 card to the latest image file:
    sysfpga_upgrade lc1
    sysfpga_upgrade lc2
    .....
    sysfpga_upgrade lc8

to upgrade sysfpga on a remote SFM s1/s2/./s6 card to the latest image file:
    sysfpga_upgrade s1
    sysfpga_upgrade s2
    .....
    sysfpga_upgrade s6

to upgrade entire chassis fpga:
    sysfpga_upgrade all

to retrieve chassis/slot/fpga info:
    sysfpga_upgrade show

to get help:
    sysfpga_upgrade help
```

4. Optional: Upgrade the FPGA firmware for the linecard (LC) using the **sysfpga_upgrade lc<slot#>** command.

The range of valid slot values is from 1 through 4 for the SLX 9850-4.

The range of valid slot values is from 1 through 8 for the SLX 9850-8.

For example:

```
# sysfpga_upgrade lc3
```

5. Optional: On the active MM, upgrade the FPGA firmware for the Switch Fabric Module (SFM) using the **sysfpga_upgrade sfm<slot#>** command.

The range of valid slot values is from 1 through 4 for the SLX 9850-4.

The range of valid slot values is from 1 through 8 for the SLX 9850-8.

For example:

```
# sysfpga_upgrade sfm3
```

- Once the FPGA upgrade is complete, issue the **exit** command to return to the privileged EXEC mode prompt.
- Reboot the chassis with the **reload system powercycle** command.

```
device# reload system powercycle
```

- Once the chassis reboots, verify the FPGA version using the **oscmd fpga version** command to ensure the version is correct. For additional information, refer to the *FPGA version mismatch correction* topic.

```
device# oscmd fpga version
```

FPGA version mismatch correction

Checks the FPGA versions on the SLX 9850 hardware family.

A version mismatch between FPGA applications and hardware results in system failure and continuous reboot on every module initialization failure. This procedure corrects FPGA version mismatch issues.

NOTE

Extreme Networks recommends that you confirm the FPGA version after doing an upgrade or downgrade between firmware releases.

- Execute the **oscmd FPGA version** command. Verify that the dates shown in the "Version" column match the dates shown in the "Latest Version" column.

```
device# oscmd fpga version
+-----+-----+-----+-----+
| Blade | Version | Type | Latest Version |
+-----+-----+-----+-----+
| MM1 | 08/25/2016 (52) | 2001 | 8/25/2016 |
+-----+-----+-----+-----+
| MM2 | 08/25/2016 (52) | 2001 | 8/25/2016 |
+-----+-----+-----+-----+
| LC1 | 08/30/2016 (54) | 2017 | 8/30/2016 |
+-----+-----+-----+-----+
| LC2 | 08/30/2016 (54) | 2017 | 8/30/2016 |
+-----+-----+-----+-----+
| LC3 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC4 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC5 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC6 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC7 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC8 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| SFM1 | 05/25/2016 (48) | N/A | 8/04/2016 | <=====Example here
+-----+-----+-----+-----+
| SFM2 | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM3 | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM4 | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM5 | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM6 | Vacant | N/A | N/A |
+-----+-----+-----+-----+
```

- If the versions do not match, log into the SLX via the SSH or serial console as an administrator.

- Execute the **start-shell** command.
- Perform the steps in the SLX-9850 fpga upgrade section. Execute the **sysfpga_upgrade <option>** command, where the option is selected from the list below.

```
# sysfpga_upgrade help
===== Fusion Sysfpga Upgrading Help Page =====
to upgrade sysfpga on local MM card to the latest image file:
    sysfpga_upgrade mm

to upgrade sysfpga on a remote F4 LC lc1/lc2/lc3/lc4 card to the latest image file:
    sysfpga_upgrade lc1
    sysfpga_upgrade lc2
    sysfpga_upgrade lc3
    sysfpga_upgrade lc4

to upgrade sysfpga on a remote F8 LC lc1/lc2/./lc8 card to the latest image file:
    sysfpga_upgrade lc1
    sysfpga_upgrade lc2
    .....
    sysfpga_upgrade lc8

to upgrade sysfpga on a remote SFM s1/s2/./s6 card to the latest image file:
    sysfpga_upgrade s1
    sysfpga_upgrade s2
    .....
    sysfpga_upgrade s6

to upgrade entire chassis fpga:
    sysfpga_upgrade all

to retrieve chassis/slot/fpga info:
    sysfpga_upgrade show

to get help:
    sysfpga_upgrade help
```

- Once the FPGA upgrade is complete, issue the **exit** command to return to the privileged EXEC mode prompt.
- Execute the **reload system powercycle** command to reboot the device.

- Once the chassis is back online, connect and execute the **oscmd FPGA version** command. Verify that the dates shown in the "Version" column match the dates shown in the "Latest Version" column.

```

device# oscmd fpga version
+-----+-----+-----+-----+
| Blade | Version | Type | Latest Version |
+-----+-----+-----+-----+
| MM1   | 08/25/2016 (52) | 2001 | 8/25/2016 |
+-----+-----+-----+-----+
| MM2   | 08/25/2016 (52) | 2001 | 8/25/2016 |
+-----+-----+-----+-----+
| LC1   | 08/30/2016 (54) | 2017 | 8/30/2016 |
+-----+-----+-----+-----+
| LC2   | 08/30/2016 (54) | 2017 | 8/30/2016 |
+-----+-----+-----+-----+
| LC3   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC4   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC5   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC6   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC7   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| LC8   | Vacant | N/A | N/A |
+-----+-----+-----+-----+
| SFM1  | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM2  | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM3  | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM4  | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM5  | 08/04/2016 (50) | N/A | 8/04/2016 |
+-----+-----+-----+-----+
| SFM6  | Vacant | N/A | N/A |
+-----+-----+-----+-----+

```

SLX 9540 fpga upgrade

This procedure updates the fpga (Field Programmable Gate Array) flash with the latest image from the installation package.

- Confirm the peripheral firmware requires an upgrade using the **show firmware peripheral fpga** command. If the dates are not identical, the firmware must be upgraded.

```

device# show firmware peripheral fpga
+-----+-----+-----+-----+
| Type | Current Version | Latest Version Available |
+-----+-----+-----+-----+
| sysfpga | 02/09/2017 (92) | 02/09/2017 (92) |
+-----+-----+-----+-----+

```

- Update the firmware using the **firmware peripheral-update fpga** command.

```

device# firmware peripheral-update fpga
erasing .. .. done
programming ..... 25% ..... 50% .....
75% ..... 100
sysfpga image is upgraded successfully.

```

3. Reboot the device using the **reload system** command.

```
device# reload system
```

SLX 9540 CPLD image upgrade

Updates the Complex Programmable Logic Device (CPLD) flash with the latest image from the installation package.

1. Confirm the peripheral firmware requires an upgrade with the **show firmware peripheral cpld** command. If the dates are not identical, the firmware must be upgraded.

```
device# show firmware peripheral cpld
+-----+-----+-----+
| Type      | Version      | Latest Version |
+-----+-----+-----+
| cpld0     | 09/25/2016(92) | 9/26/2016(92) |
+-----+-----+-----+
| cpld1     | 09/25/2016(92) | 8/26/2016(92) |
+-----+-----+-----+
```

2. Update the firmware with the **firmware peripheral-update cpld** command. Both units are upgraded automatically.

```
device# firmware peripheral-update cpld
erasing .... done
programing ..... 25% ..... 50% ..... 75% ..... 100%
cpld0 image is upgraded successfully.
```

```
erasing .... done
programing ..... 25% ..... 50% ..... 75% ..... 100%
cpld1 image is upgraded successfully.
```

3. Reboot the device with the **reload system** command.

```
device# reload system
```

4. Confirm the units were upgraded with the **show firmware peripheral cpld** command. The dates should be identical.

```
device# show firmware peripheral cpld
+-----+-----+-----+
| Type      | Current Version| Latest Version |
+-----+-----+-----+
| CPLD0     | 02/09/2017(92) | 02/09/2017(92) |
+-----+-----+-----+
| CPLD1     | 02/09/2017(92) | 02/09/2017(92) |
+-----+-----+-----+
```

Upgrading devices with BGP neighbor send-community configuration

Consider the following when upgrading devices with BGP **neighbor send-community** configurations.

Upgrading to the SLX-OS 18r.2.00 software version has behavioral changes that affect the running configuration and the startup configuration for devices with **neighbor send-community** configurations under the following BGP address-family configuration modes.

- **address-family ipv4 unicast [vrf vrf-name]**
- **address-family ipv6 unicast [vrf vrf-name]**

- **address-family vpnv4 unicast**
- **address-family vpnv6 unicast**

For SLX-OS 18r.1.00 and earlier releases, the previously-listed BGP **address-family** configurations support the following **neighbor send-community** command:

```
neighbor { ip-address | ipv6-address | peer-group-name } send-community [ both | extended | standard ]
```

Starting with SLX-OS 18r.2.00 release, the **neighbor send-community** configuration in the previously-listed address-family modes supports the additional **all** and **large** options:

```
neighbor { ip-address | ipv6-address | peer-group-name } send-community [ all | both | extended | large | standard ]
```

The introduction of the **large** keyword in the **neighbor send-community** configuration has changed the meaning of the **both** keyword that used to refer to both the **standard** and **extended** community options.

NOTE

Starting with SLX-OS 18r.2.00, it is advised not to use the **both** keyword for the previously-listed BGP **address-family** configuration, even though the configuration is supported. Using the **both** keyword continues to refer to **standard** and **extended** community options.

With this in mind, upgrading to the SLX-OS 18r.2.00 software version has behavioral changes that pertain to the running configuration and the startup configuration for devices with the **neighbor send-community** configuration. If the old startup configuration is used when upgrading, all references to the **both** keyword in the startup configuration for the previously-listed BGP **address-family** configurations expand into two configuration statements with the **standard** and **extended** keywords in the running configuration.

The following example shows the old BGP startup-config:

```
show startup-config
...
address-family ipv4 unicast
neighbor 192.168.1.10 send-community both
...
```

The following example shows the new BGP running-config:

```
show running-config
...
address-family ipv4 unicast
neighbor 192.168.1.10 send-community standard
neighbor 192.168.1.10 send-community extended
...
```

Additionally, the **all** keyword introduced in SLX-OS 18r.2.00 can be used to configure all three communities (standard, extended, and large) for the neighbor.

Downgrading considerations and restrictions

Consider the following when downgrading your firmware version:

- If a feature is new for the current version of your firmware, it does not function if you downgrade your firmware version.
- Firmware downgrades to previous versions are prohibited when security parameters are configured for HTTPS support.
- CFM configurations are not compatible with versions prior to SLXR 17r.2.01.
- If you are downgrading from a 64-bit to a 32-bit system, use the **fullinstall** option when you execute the **firmware download** command.

- Before downgrading to a version that doesn't support RADIUS accounting, both login and command accounting must be disabled.
- Before downgrading to a version that doesn't support RADIUS accounting, the source interface for the RADIUS configuration must be removed.

Always refer to the release notes for compatibility information and take note of restrictions that may exist regarding upgrades and downgrades under particular circumstances.

SLX-OS Capabilities

- Viewing software capabilities..... 31

Viewing software capabilities

To display information about the software capabilities, enter the **show license** command. The command output displays the currently installed licenses for Extreme SLX-OS.

For example:

```
device# show license
Slot 1
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Port Upgrade license
Feature name:PORT_100G_40G_UPGRADE
Capacity: 30x100G or 50X40G
License is Node-Lock and valid
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
MPLS license
Feature name: MPLS
License is Node-Lock and valid
Slot 2
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Port Upgrade license
Feature name:PORT_10G_UPGRADE
Capacity: 36x10G
License is Node-Lock and valid
```

SLX 9640 device example:

```
device# show license
Chassis:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    100G Port Upgrade license
    Feature name:PORT_100G_UPGRADE
    Capacity: 8
    License is Node-Lock and valid
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Advanced Features license
    Feature name:ADVANCED_FEATURES
    License is Trust Based
    EULA acceptance date: Thu Aug 23 02:13:08 2018
```