Extreme™
Customer-Driven Networking

Extreme SLX-OS
Software Upgrade Guide, 16r.1.01

Supporting the ExtremeRouting SLX 9850 Router

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme technical documentation.

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.
`Courier font`	Identifies CLI output.

Format	Description
	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.

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you.

You can provide feedback in two ways:

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

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.

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

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

- GTAC (Global Technical Assistance Center) for immediate support
    - Phone: 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.
    - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

About This Document

What's new in this document

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.

The following tables include descriptions of new information added to this guide for this release of Extreme SLX-OS.

TABLE 1 Summary of enhancements

Feature	Description	Described in
FPGA version check	Process for correcting FPGA version mismatch issues.	Installing and Maintaining Firmware

Supported hardware and software

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 and which are not.

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for SLX-OS Release 16r.1.01, 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
- ExtremeRouting SLX 9850-8

Installing and Maintaining Firmware

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.

Upgrading firmware on a modular chassis

In SLX OS 16r.1.01 in-service software upgrade (ISSU) is not supported.

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.

Supported platforms

The following lists supported firmware versions by platform.

TABLE 2 SLX-OS firmware support by platform

Platform	16r.1.00	16r.1.01
Extreme SLX 9850-4 Router	yes	yes
Extreme SLX 9850-8 Router	yes	yes

Self Authenticated Upgrade license management

The Self Authenticated Upgrade (SAU) license enables the advanced licensed feature set prior to purchasing a license.

The SAU license does not require an activation process or transaction key. You do not need to install a physical license on the SLX-OS platform to use the licensed feature set. The EULA requires a license to be purchased within 30 days of accepting the license EULA statement through the CLI. A Certificate of Entitlement (CoE) is issued through Extreme once you have paid for SAU license. The CoE document certifies that you have paid for the license to use the feature for a specific platform.

You must accept the End-User License Agreement (EULA) through the CLI commands before the system can support the licensed capabilities. Once you accept the EULA, you can configure and begin using the feature on the device.

The following example displays the EULA text.

```
device# show license eula
Use of the features enabled via the "license eula accept" CLI requires a license to
be purchased within 30 days. By accepting the EULA you indicate that you
have read and accept the Brocade End User License Agreement found at the following URL.
[www.brocade.com/en/legal/software-terms-eulas/brocade-network-operating-system.html].
```

When the **license eula accept** command is entered, you are agreeing to purchase a license within a specific time frame. You can begin using the features immediately.

The following example shows how to accept the EULA for the SAU license (Advanced Features).

```
device# license eula accept ADVANCED_FEATURES
2016/12/05-13:35:00, [SEC-1120], 64,, INFO, SLX9540, License EULA entry added for ADVANCED_FEATURES feature
(capacity 0).

EULA accepted for feature [ADVANCED_FEATURES]

Use of the ADVANCED_FEATURES feature requires a license to be purchased within 30 days.
By accepting the EULA you indicate that you have read and accept the Brocade End User License Agreement
found at the following URL
[www.brocade.com/en/legal/software-terms-eulas/brocade-network-operating-system.html].
You can decline the EULA acceptance now by entering "license eula decline ADVANCED_FEATURES"
at the CLI prompt; declining the EULA will prevent use of the licensed feature.
```

The **show license** command will also display the SAU license when the EULA is accepted.

```
device# show license
Chassis:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Advanced Features license
Feature name:ADVANCED_FEATURES
License is Trust Based
EULA acceptance date: Mon Dec  5 13:35:00 2016
```

When the **license eula decline** command is entered, you are no longer able to use the licensed features. Before you can "decline" the licensed features, all configuration settings related to the feature must be restored to default settings.

The following CLI message is displayed when you attempt to configure a feature that requires a SAU license, and you have not accepted the EULA and there is no SAU license installed for that feature.

```
No ADVANCED_FEATURES EULA accepted for this feature
```

Preparing for a Firmware Download

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 18.

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 15.

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 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 an FTP or SCP variant server and decompress the package *before* you can use the **firmware download** command to upgrade the firmware on your equipment.

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.

Five **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.

- noactivate: Downloads the firmware to the system without activating it, so the device is not automatically rebooted.
- nocommit: Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition.
- noceboot: Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually.

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.

Basic Firmware Upgrade

Connecting to the router

When you upgrade firmware in default mode, you connect to the router through the management IP address. Modular routers have one management IP address for the chassis and separate IP addresses for each management module. To upgrade both management modules, you can either connect to the chassis management IP address or to the IP address of the active management module. If you want to upgrade a single management module only, you must connect to the IP address of that management module and run the **firmware download** command in manual mode. In manual mode, only the local management module is upgraded.

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

```
device# show system
Stack MAC                       : 00:05:33:15:FA:70
  -- UNIT 0 --
Unit Name                       : sw0
Switch Status                   : Online
Hardware Rev                    : 1000.0
TengigabitEthernet Port(s)      : 56
Up Time                         : up 8:38
Current Time                    : 16:39:56 GMT
SLX Version                     : 16r.1.01
Jumbo Capable                   : yes
Burned In MAC                   : 00:05:33:15:FA:70
Management IP                   : 10.xx.xx.131 <- Chassis Management IP address
Management Port Status          : UP
```

Use the **show interface management** command to display the IP addresses for the management modules.

```
device# show interface management
interface Management 10/1
 ip address 10.xx.xx.130/20
 ip gateway-address 10.xx.xx.1
 ipv6 ipv6-address [ ]
 ipv6 ipv6-gateways [ ]
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
interface Management 10/2
 ip address 10.xx.xx.23/20
 ip gateway-address 10.xx.xx.1
 ipv6 ipv6-address [ ]
 ipv6 ipv6-gateways [ ]
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
```

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

Upgrading firmware on a local device

A basic firmware download upgrades the local device only. This section explains how to use the **firmware download** command and its various options in a local device firmware upgrade.

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.

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) 2014-2017 Brocade COmmunications, 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        ACTIVE*
                 17r.1.00slxos_17r.1..x_maint_160819_1858

 device# show version

SLX-OS Operating System Software
SLX-OS Operating System Version: 17s.1.00
Copyright (c) 2014-2017 Brocade COmmunications, Inc.
Firmware name:      17s.1.00_bfd_fix
Build Time:         23:24:03 Mar  3, 2017
Install Time:       18:54:34 Mar  4, 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:    1days 19hrs 40mins 54secs

Slot     Name    Primary/Secondary Versions                     Status
---------------------------------------------------------------------
SW/0     SLX-OS  17s.1.00.x_maint_160819_1858                   ACTIVE*
                 17s.1.00.x_maint_160819_1858
```

Using the firmware download command

Two upgrade options are available:

- Coldboot - Coldboot is the standard option for dual-MM system for all firmware upgrades between major releases.
- Default-config - Removes all configuration and is similar to an initial installation and configuration.

  NOTE
  To be able to address the FTP 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 & ! % #) in FTP and SCP passwords. If your SCP or FTP password contains special characters, the download fails.

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

   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                                   ACTIVE*
                17s.1.0017s.1.00
```

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                                    ACTIVE*
                17r.1.0017r.1.00

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                                    ACTIVE*
                17s.1.0017s.1.00
```

SLX-OS Capabilities

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.

```
device# show license
Chassis:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
        Advanced Features license
        Feature name:ADVANCED_FEATURES
        License is Trust Based
        Eula date is Tue Mar 14 16:54:59 2017

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