

39XX/51XX Switches and Platforms

Software Management and Licensing

SAOS 6.21.2

What's inside...

New in this release

Software management fundamentals

Software license fundamentals

Managing system software

Managing software license keys

Live patching

009-3458-018 - Standard Revision A

March 2022

Copyright© 2022 Ciena® Corporation. All rights reserved.

LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing CIENA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit www.ciena.com.

Copyright© 2022 Ciena® Corporation. All Rights Reserved

Use or disclosure of data contained in this document is subject to the Legal Notices and restrictions in this section and, unless governed by a valid license agreement signed between you and Ciena, the Licensing Agreement that follows.

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

Contacting Ciena

Corporate Headquarters	410-694-5700 or 800-921-1144	www.ciena.com
Customer Technical Support/Warranty		www.ciena.com/support/
Sales and General Information	North America: 1-800-207-3714 International: +44 20 7012 5555	E-mail: sales@ciena.com
In North America	410-694-5700 or 800-207-3714	E-mail: sales@ciena.com
In Europe	+44-207-012-5500 (UK)	E-mail: sales@ciena.com
In Asia	+81-3-3248-4680 (Japan)	E-mail: sales@ciena.com
In India	+91-22-42419600	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training		E-mail: learning@ciena.com

For additional office locations and phone numbers, please visit the Ciena web site at www.ciena.com.



READ THIS LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE INSTALLING OR USING CIENA SOFTWARE OR DOCUMENTATION. THIS LICENSE IS AN AGREEMENT BETWEEN YOU AND CIENA COMMUNICATIONS, INC. (OR, AS APPLICABLE, SUCH OTHER CIENA CORPORATION AFFILIATE LICENSOR) ("CIENA") GOVERNING YOUR RIGHTS TO USE THE SOFTWARE. BY INSTALLING OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND AGREE TO BE BOUND BY IT.

1. License Grant. Ciena may provide "Software" to you either (1) embedded within or running on a hardware product (together with Software, "Product") or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. The terms of this License apply to your use of the Software and associated documentation whether such has been provided by Ciena, an affiliate of Ciena, or by means of an authorized reseller or distributor. Subject to these terms, and payment of all applicable License fees including any usage-based fees, Ciena grants you, as end user, a non-exclusive, non-transferable, personal License to use the Software only in object code form, subject to any applicable authorized use, activation requirements, usage levels, scope of functionality and release level of the Software, as set forth in the applicable quote accepted by Buyer upon Buyer's issuance of an acceptable purchase order ("Order"), and in accordance with the detailed ordering information in the Ciena's generally available, applicable, Product documentation as of the date of such Order. Unless the context does not permit, Software also includes associated documentation. Where an Order is for a (a) perpetual license, you may use the Software and associated documentation for as long as you use the Product for internal business use, or a (b) subscription license, you may only use the Software and associated documentation during the subscription term. A subscription license includes Software upgrades and/or technical support Services during the subscription term (that are not included in a perpetual license), in accordance with the Order and as further described in the applicable Ciena's service description as of the date of the applicable Order. Prior to the expiration of each subscription term, Ciena will send you a quote for the annual renewal fee(s). To renew the subscription Software license(s) for additional subscription terms, you issue an Order in advance of the then-current expiration date of such subscription term.

2. Open Source and Third-Party Licenses. If any Software is subject to an open-source license that provides the end user with rights that are broader than this License, then such rights shall take precedence. Ciena warrants that using Software in accordance with its documentation will not subject you to any obligation to disclose, distribute or license your own software that interacts with Software.

3. Title. You are granted no title or ownership rights in or to the Software. Unless specifically authorized by Ciena in writing, you are not authorized to create any derivative works based upon the Software. Title to the Software, including any copies or derivative works based thereon, and to all copyrights, patents, trade secrets and other intellectual property rights in or to the Software, are and shall remain the property of Ciena and/or its licensors. Ciena's licensors are third party beneficiaries of this License. Ciena reserves to itself and its licensors all rights in the Software not expressly granted to you.

4. Confidentiality. The Software contains trade secrets of Ciena. Such trade secrets include, without limitation, the design, structure and logic of individual Software programs, their interactions with other portions of the Software, internal and external interfaces, and the programming techniques employed. The Software and related technical and commercial information, and other information received in connection with the purchase and use of the Software that a reasonable person would recognize as being confidential, are all confidential information of Ciena ("Confidential Information").

5. Obligations. You shall:

- i) Hold the Software and Confidential Information in strict confidence for the benefit of Ciena using your best efforts to protect the Software and Confidential Information from unauthorized disclosure or use, and treat the Software and Confidential Information with the same degree of care as you do your own similar information, but no less than reasonable care;
- ii) Keep a current record of the location of each copy of the Software you make;
- iii) Use the Software only in accordance with the authorized usage level;
- iv) Preserve intact any copyright, trademark, logo, legend or other notice of ownership on any original or copies of the Software, and affix to each copy of the Software you make, in the same form and location, a reproduction of the copyright notices, trademarks, and all other proprietary legends and/or logos appearing on the original copy of the Software delivered to you; and
- v) Issue instructions to your authorized personnel to whom Software is disclosed, advising them of the confidential nature of the Software and provide them with a summary of the requirements of this License.

6. Restrictions. You shall not:

- i) Use the Software or Confidential Information a) for any purpose other than your own internal business purposes; and b) other than as expressly permitted by this License;
- ii) Allow anyone other than your authorized personnel who need to use the Software in connection with your rights or obligations under this License to have access to the Software;
- iii) Make any copies of the Software except such limited number of copies, in machine readable form only, as may be reasonably necessary for execution in accordance with the authorized usage level or for archival purposes only;
- iv) Make any modifications, enhancements, adaptations, derivative works, or translations to or of the Software;
- v) Reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Software;
- vi) Make full or partial copies of the associated documentation or other printed or machine-readable matter provided with the Software unless it was supplied by Ciena in a form intended for reproduction;
- vii) Export or re-export the Software and/or the associated documentation from the country in which it was received from Ciena or its authorized reseller unless authorized by Ciena in writing; or
- viii) Publish the results of any benchmark tests run on the Software.

7. Audit: Upon Ciena's reasonable request you shall permit Ciena to audit the use of the Software to ensure compliance with this License.

8. U.S. Government Use. The Software is provided to the Government only with restricted rights and limited rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in FAR Sections 52-227-14 and 52-227-19 or DFARS Section 52.227-7013(C)(1)(ii), as applicable. The Software and any accompanying technical data (collectively "Materials") are commercial within the meaning of applicable Federal acquisition regulations. The Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this License, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, the Software is commercial computer software and the use of the Software is further restricted by this License.

9. Term of License. This License is effective until the applicable subscription term expires or the License is terminated. You may terminate this License by giving written notice to Ciena. This License will terminate immediately if (i) you breach any term or condition of this License or (ii) you become insolvent, cease to carry on business in the ordinary course, have a receiver appointed, enter into liquidation or bankruptcy, or any analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. Upon any termination of this License, you shall destroy and erase all copies of the Software in your possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased. Your obligations to hold the Confidential Information in confidence, as provided in this License, shall survive the termination of this License.

10. Compliance with laws. You agree to comply with all laws related to your installation and use of the Software. Software is subject to U.S. export control laws and may be subject to export or import regulations in other countries. If Ciena authorizes you to import or export the Software in writing, you shall obtain all necessary licenses or permits and comply with all applicable laws.

11. Limitation of Liability. ANY LIABILITY OF CIENA SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU TO CIENA OR ITS AUTHORIZED RESELLER FOR THE SOFTWARE. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, INCLUDING WITHOUT LIMITATION BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS. THE LIMITATIONS OF LIABILITY DESCRIBED IN THIS SECTION ALSO APPLY TO ANY LICENSOR OF CIENA. NEITHER CIENA NOR ANY OF ITS LICENSORS SHALL BE LIABLE FOR ANY INJURY, LOSS OR DAMAGE, WHETHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, CONTRACTS, DATA OR PROGRAMS, AND THE COST OF RECOVERING SUCH DATA OR PROGRAMS, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12. General. Ciena may assign this License to an affiliate or to a purchaser of the intellectual property rights in the Software. You shall not assign or transfer this License or any rights hereunder, and any attempt to do so will be void. This License shall be governed by the laws of the State of New York without regard to conflict of laws provisions. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This License constitutes the complete and exclusive agreement between the parties relating to the license for the Software and supersedes all proposals, communications, purchase orders, and prior agreements, verbal or written, between the parties. If any portion hereof is found to be void or unenforceable, the remaining provisions shall remain in full force and effect.

Publication history

March 2022

First Standard release of this document for SAOS 6.21.2.

Contents

About this document	ix
Software management fundamentals	2-1
Overview	2-1
Network connectivity and xFTP server settings	2-2
System software package	2-2
File naming conventions	2-3
Upgrade paths	2-4
xFTP package directory	2-4
Command files	2-6
Command file types	2-6
Software license fundamentals	3-1
Managing system software	4-1
Types of resets	4-1
List of procedures	
4-1 Specifying xFTP server settings	4-3
4-2 Transferring files	4-7
4-3 Upgrading using the CLI and a command file	4-9
4-4 Upgrading using the CLI without a command file	4-12
4-5 Upgrading using a DHCP server	4-16
4-6 Upgrading using the software install command	4-18
4-7 Upgrading the SFP packet processor	4-21
4-8 Downgrading the SFP packet processor	4-23
4-9 Upgrading the TDM module packet processor	4-24
4-10 Downgrading the TDM module packet processor	4-25
4-11 Activating the software	4-26
4-12 Generating sequence reports	4-27
4-13 Backing up software images	4-30
4-14 Displaying board support and datapath FPGA version information	4-31
Managing software license keys	5-1
List of procedures	
5-1 Installing a license key	5-2
5-2 Installing a license key using a license file	5-4

- 5-3 Installing a license key file with the command file 5-7
 - 5-4 Uninstalling a license key 5-8
-

Live patching

6-1

- Deployment 6-2
- Live patch unit file deactivation and removal 6-3
- Live patch unit queries 6-3
- Limitations 6-3

List of procedures

- 6-1 Adding a live patch unit file to the patch database 6-4
- 6-2 Removing a patch 6-5
- 6-3 Modifying the state of the patch 6-6
- 6-4 Displaying patches 6-7

About this document

This document describes software management and licensing on 39XX/51XX Switches and Platforms. This system software is based on a common Service Aware Operating System (SAOS) code base designed to deliver consistent benefits across all Ethernet delivery, aggregation, and distribution configurations.

Note: This system software cannot be installed on Service Delivery Switches, Service Concentration Switches or Service Aggregation Switches other than 39XX/51XX switches.

This document provides information and examples for use in configuring system software on any switch on which it is installed. It includes an explanation of the key features supported by the devices and provides example configurations for these features. Although these examples are useful in configuration, they are not meant to be used as a configuration template.

Conventions used in this document

Hyperlinks are indicated by [blue](#) text in this document.

In procedures, the following text conventions are used:

- `courier` text, for system responses
- *italic* text, for expected results
- **bold** text, for user input

Command syntax

A variety of symbols are used to indicate CLI command syntax. These symbols describe how to enter a command. They are not entered as part of the command itself. The following table summarizes command syntax symbols.

Symbol	Description
< >	Encloses a variable or literal value that must be specified. Some examples include: server <IpAddress> priority <NUMBER: 1-7> dns <on off> description <String[31]> For server <IpAddress>, the attribute could be entered as server 10.10.11.100 or server www.ciena.com. With priority <NUMBER: 1-7> the text within <> indicates that 1 - 7 are valid values. In the example of dns <on off>, either the literal value of on or off is valid, such as dns on. For description <String[31]>, any string of up to 31 characters is entered.
{ }	Encloses a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax: cfm mip create {vlan <VlanId>} {port <PortNameList>} [level <NUMBER: 0-7>] The vlan and port arguments are required. The level argument is optional.
	Separates mutually exclusive items in a list, only one of which can be entered. For example, in the syntax: dhcp client options set subnet <on off> Either on or off must be specified, for example: dhcp client options set subnet on
[]	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax: arp show [interface <Interface>] You can enter a value for interface <Interface> or not. For example: arp show

Symbol	Description
{ [], [], [] }	Specifies a list of optional items where at least one must be specified.
...	Indicates the example has been abbreviated and that the actual display contains more information.
*	Indicates zero or more occurrences of what is preceding.

Documents in the 39XX/51XX documentation suite

For descriptions of documents in the 39XX/51XX Switches and Platforms documentation suite, see *39XX/51XX Switches and Platforms Product Fundamentals*.

New in this release

This section provides a summary of the changes made in *39XX/51XX Switches and Platforms Software Management and Licensing* for SAOS 6.21.2.

- The *<encrypted-password-attr>* command is removed from the system and all instances of this command is deleted from all procedures in this guide, primarily impacted in the following sections:
 - [Procedure 4-1, “Specifying xFTP server settings”](#)
 - [Procedure 4-2, “Transferring files”](#)

Software management fundamentals

This chapter describes software management for upgrading and downgrading 39XX/51XX Switches and Platforms.

Overview

Software upgrades and downgrades can be performed from the CLI, SNMP, or by running command files. The upgrade process takes about 10 minutes to complete. Upgrades for multiple switches in a network should take place in an organized manner, for example, starting from the edge of the network and working toward the core, or starting from the core and working toward the edge.

From the user interface perspective, there is no difference between upgrade and downgrade. The same commands are used in both cases. The term X-grade is used to mean upgrade or downgrade.

Note: Certain switches may not have the latest released software and require an upgrade after initial installation to support desired features.

When a device is upgraded or downgraded to a different software package version, the new software package may contain different board support enhanced port firmware and different SAOS software. If the new board support enhanced port firmware version differs from the version running on the device, the board support enhanced port firmware will be upgraded or downgraded. When the device is rebooted, it reboots twice. One reboot installs the new board support enhanced port firmware and the other installs the new SAOS software. The extra reboot is not noticeable unless you are watching the console or the timing of the upgrade process.

Software management comprises the following options:

- **Software install** — Software can be installed without becoming activated. A running package is software that is currently active. The user can specify if they want the installed software to be loaded on the next reboot.
- **Software upgrade** — Upgrades software from one release to another. Once the software package is downloaded, the software is activated to become the running package.

- **Software activate** — The software activate command validates previously installed software and uses that software version for the next boot. This command allows the user to choose whether it is service disrupting. This command fails if the user attempts to activate an invalid bank or the package does not exist on the device. A software activate can be used to cancel a previously executed install or activate by specifying the currently running bank.
- **Software protect** — When switches have two flash banks of A and B and the running flash bank fails, the standby bank takes over. The software protect command ensures that there are identical software versions on the two banks. Therefore, if one bank fails, the standby bank takes over and runs the identical software.
- **Software validate** — The software validate command validates the status of the standby bank and checks for its integrity. Some switches take longer than others. The command generally takes less than 30 seconds to execute.

Network connectivity and xFTP server settings

The system software X-grade process requires the device to have network connectivity in order to download files and send notifications. The serial console, the local interface, or remote interface can be used for the X-grade, but the interface must be configured properly before the X-grade is started. Refer to the “Turning up the system” chapter in the switch’s Installation Manual for interface configuration details. Specifically, the device must be able to communicate with a File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or Secure File Transfer Protocol (SFTP) server, which is referred to as the xFTP server, and optionally, the Syslog server and SNMP trap server.

System software package

The system software is released in the form of a software package ZIP file, containing the files summarized in [Table 2-1](#).

Table 2-1
Software Package Files

File Name	Description
mibs <dir>	Complete MIB set for device management
le-<Image ID>-caliondo_nand.tar.xz	Complete set of image files for 3942 and 5142 switches. Partial image files for 5160.
le-<Image ID>-dernhelm.tar.xz	Complete set of image files for 3903, 3903x, 3904, 3905 and 3906 switches.
le-<Image ID>-eredan.tar.xz	Complete set of image files for 3926 and 3928 switches.
le-<Image ID>-5160.tar.gz	Backwards-compatible image files for 5160 switch.
le-<Image ID>-cavium.ins	Upgrade install script for 3942, 5142 and 5160 switches.
le-<Image ID>-dernhelm.ins	Upgrade and install script for 3903, 3903x, 3904, 3905 and 3906 switches.
le-<Image ID>.chk	Upgrade check script for all switches,
le-lnx.xml	Software command file
pmf-saos-<build>.xml	Package metafile
mainShellMenu.xml	Command Line Interface syntax definition
mainShellMenu.xsl	Command Line Interface XML grammar
readme.txt	Package readme file

File naming conventions

The package name follows the naming convention of “saos-AA-BB-CC-DDDD.”

where

AA	major version number
BB	minor version number
CC	maintenance version number
DDDD	build number

Upgrade paths

Ciena supports planning and evolution of customer networks with a strategy of N±2 release upgrade path compatibility among major releases of SAOS software. This means, for example, that 39xx/51xx devices can migrate between 6.15.x and 6.17.x releases with minimal disruption to normal operation.

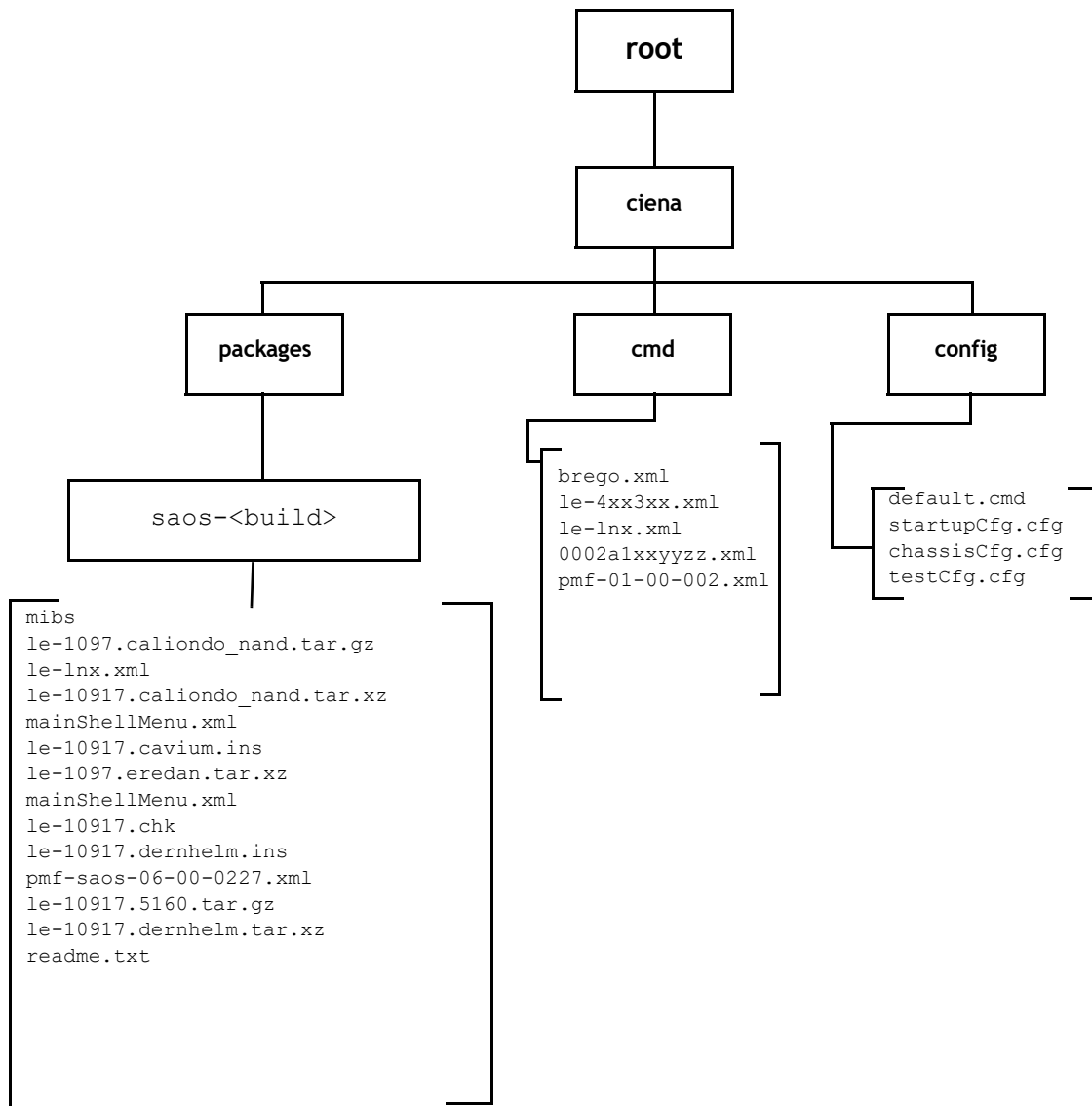
Introduction of new capabilities in minor and path SAOS releases necessarily means that some migration paths require associated implementation notes. For relevant details, always refer to the section “Upgrade and downgrade considerations” in the *Customer Release Notes* for the release you are targeting.

Note: Ciena tests migration paths on a variety of 39xx/51xx devices in a variety of representative network configurations. Network and feature configurations differ widely, and some may present special circumstances. If you experience difficulty in following a supported migration path, contact your Ciena support representative for guidance.

xFTP package directory

The software package ZIP file is created so that all files will be extracted to a sub-directory named saos <build> directory on the xFTP server (where <build> is the actual build number of the system software, for example, saos-06-14-00-XXXX). The recommended file structure for the xFTP package directory is <xftpboot>/ciena/packages/ (where <xftpboot> is a sub-directory of the server root designated for xFTP, such as “tftp”).

Figure 2-1
Sample xFTP Directory Structure



In [Figure 2-1](#), the root directory refers to the root directory for the xFTP server. Operators are free to define the root directory however they wish. All files and directories are stored in one subdirectory off the root directory named “ciena”. This directory has three subdirectories:

- **packages:** This directory has one subdirectory for each software package. Each directory contains all the image files for all device types supported by the software package. This directory also contains switch or board capability files. File names may be changed, but the extensions may not be changed (such as .xml).

- `cmd`: Device command files. This directory contains command files and package meta files for each switch class. Command files for specific devices may also exist in this directory, such as `<MACaddress>.xml`.
- `config`: This directory contains configuration files such as `startup-config`, `chassis-config`, etc.

Command files

The software package contains a generic switch class command file named `le-ln.xml`. This is a fully functional sample command file that does not require any modifications in order to upgrade the software package on the device. Command files can also be used to install packages or configure one or more devices.

Command file types

You can use the sample command file to create additional command files for specific devices or switch classes. Device specific command files are named with the device MAC address, such as:

- `0002a1010203.xml`

Switch class command files are named as follows:

- `caliondo.xml` - for 3942, 5142 and 5160 switches
- `dernhelm.xml` - for 3903, 3903x, 3904, 3905 and 3906 switches
- `eredan.xml` - for 3926 and 3928

Customer files can be created for specific switch classes to select specific models where the file name and switch class attribute is: 3903, 3903x, 3904, 3905, 3906, 3926, 3928, 5142 and 5160. The following is an example of the `le-ln.xml` file.

```
<!--
```

```
README:  SAOS Command File
```

```
This is a sample command file.
```

```
This file will activate package saos-<build> on your device(s).
```

```
You can modify this file, rename it, and copy it as you wish.
```

```
Command files are used to install new software and/or load new configuration
files to one or many devices.  Definitions in the command file are organized
by switch-class.  You may define as many switch classes as you like
in a single command file.
```

The following example defines two switch classes and uses all possible attributes:

```
<XmlWwpCommandFile>
  <XmlCmdPlatformClass name="CN3942"
    loginBanner="mySftpLoginBannerFile.txt"
    welcomeBanner="mySftpWelcomeBannerFile.txt"
    version="saos-<build>"
    operation="upgrade"
    serviceAffecting="yes">
  </XmlCmdPlatformClass>
  <XmlCmdPlatformClass name="caliondo"
    configFilePath="myFolder/my-config-file.txt"
    configFileRule="activate"
    welcomeBanner="myBannerFile.txt"
    licenseFile="myLicenseFile.txt"
    version="saos-<build>"
    packagePath="folder1/folder2/folder3"
    operation="install"
    serviceAffecting="no"
    ftpConfigFile="ciena/defaultFtpConfig">
    <SshKeyFile name="user1.pk2"></SshKeyFile>
    <SshKeyFile name="user2.pk2"></SshKeyFile>
    <SshKeyFile name="user3.pk2"></SshKeyFile>
  </XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

The following attribute is MANDATORY:

platformClass

In order of preference, the most specific match (eg, 3942), then the class match (eg, caliondo for 3942, 5142, and 5160), dernhelm for 3903, 3903x, 3904, 3905 and 3906, eredan for 3926 and 3928)

Possible values for platformClass:

3903, 3903x, 3904, 3905, 3906, 3926, 3928, 3942, 5142, 5160, brego, caliondo, dernhelm, eredan.

The following attributes are OPTIONAL:

configFilePath	(path and filename, path is relative to the file server's root directory)
configFileRule	(see note #1 below)
loginBanner	(path and filename, path is relative to to the file server's root directory)
welcomeBanner	(path and filename, path is relative to the file server's root directory)
licenseFile	(path and filename, path is relative to to the file server's root directory)
SshKeyFile	(path and filename, path is relative to to the file server's root directory)
version	(saos-xx-yy-zz-abcd)
packagePath	(complete path to the package directory relative to the to the file server's root directory)
operation	(upgrade or x-grade or install)
serviceAffecting	(yes or no)
ftpConfigFile	(path and filename, path is relative to the initial file

2-8 Software management fundamentals

server's root directory

When running the command file from the CLI, the file may be downloaded from a server using TFTP, FTP or SFTP. When using DHCP to run the command file, the command file may be specified in either option 67 (Bootfile name) or option 125 (Vendor-Identifying Vendor-Specific Information). If option 67 is used, the command file is downloaded from the TFTP server specified in option 66 (TFTP server name). If option 125 is used, the command file is downloaded from the server specified in the Ciena Bootfile URI Sub-Option. The protocol is also specified in the Bootfile URI and may be TFTP, FTP or SFTP.

If the command file does not contain an ftpConfigFile attribute for the switch being configured, all other files specified in command file attributes for that switch will be downloaded from that same server. If an ftpConfigFile attribute is specified, then that file will also be downloaded from that initial server. All other files specified in command file attributes for the switch will be downloaded from the file server specified in the ftpConfigFile file. That file server may use TFTP, FTP or SFTP.

The file server selected for downloading all files but the command file and the ftpConfigFile is referred to in the descriptions the optional attributes above as simply the "file server".

Possible values for the attribute: configFileRule

install

- Download the config file from the server.
- Store the file in the directory '/flash0/config'.
- Store the new filename as 'default-load-file'.
- Store the new filename as 'last-config-file'.
- This file will be loaded when the device is rebooted.

activate

- Same behavior as install.
- In addition, the file is activated (loaded) immediately.
- This may require a reboot.
- Reboot will not occur unless "serviceAffecting" is specified.

augment

- Download the config file.
- Augment the current system configuration with the commands in this file.

augmentAndSave

- Download the config file.
- Augment the current system configuration with the commands in this file.
- Save the resulting configuration to the file default-save-filename.

Possible values for the attribute: operation

activateAndWait

- Activate the image files on the standby bank.

activate

- Same as activateAndWait.
- Reboot after the activation takes place.

protect

- Install the currently running image on the standby bank.

upgrade

- Download the package.
- Install image files if necessary.
- Activate the new image files.
- This operation may require a reboot.
- Reboot will not occur unless serviceAffecting="yes".

install

- Download the package.
- Install image files if necessary.
- The image will be run on the next reboot.

installDeferActivation

- Same as install only the software will not be loaded until it is activated.

x-grade

- Exact same behavior as 'upgrade'.
- It is supported for backwards compatibility with previous releases.

Possible values for the attribute: serviceAffecting

```
yes          (The device is allowed to reboot if necessary)
no           (The device is NOT allowed to reboot)
```

NOTE #1

DHCP can be used to run a command file. If a command file request comes in from DHCP, the device will run the command file only once. If another request comes in with the same command file name, the device will ignore the request from DHCP. The name of the command file is saved (last-command-file) and it may be reset by the user via the shell or SNMP. The same is true for the configuration file.

NOTE #2

The License file format is shown here. Lines may appear in any order. Any text following ! will be considered a comment. Whitespace is ignored.

```
! This is my example license file
install <license key>
uninstall <feature name>
install <license key>
```

NOTE #3

The ftpConfig file format is shown here. Lines may appear in any order. Any text following ! will be considered a comment

```
!
! Contains FTP configuration parameters
!
! Valid configurable parameters are: xFtpTransferMode, server, userid
!                                     passwd, retries, retryinterval
!                                     connectiontimeout
!
! Format: e.g.
!       xFtpTransferMode:0  0=TFTP, 1=FTP 2=SFTP
!       server:<IP address or host name>
!       userid:<user name>
!
xFtpTransferMode:1
server:10.1.1.28.62
userid:su
passwd:wwp
retries:2
retryinterval:15
connectiontimeout:65
```

```
-->
```

```
- <XmlWwpCommandFile>
  <XmlCmdPlatformClass name="brego" version="saos-<build>" packagePath="ciena/
packages/saos-<build>" operation="upgrade" serviceAffecting="yes" />
  <XmlCmdPlatformClass name="caliondo" version="saos-<build>" packagePath="ciena/
packages/saos-<build>" operation="upgrade" serviceAffecting="yes" />
</XmlWwpCommandFile>
```

Possible values for the configFileRule attribute:

- install
 - Download the config file from the server.
 - Store the file in the directory '/flash0/config'.
 - Store the new filename as 'default-load-file'.
 - Store the old file as 'last-config-file'.
 - This file will be loaded when the device is rebooted.

- activate
 - Same behavior as install.
 - In addition, the file is activated (loaded) immediately.
 - This may require a reboot.
 - Reboot does not occur unless serviceAffecting = “yes”.
- augment
 - Download the config file.
 - Augment the current system configuration with the commands in this file.
 - Configuration is NOT saved.
- augmentAndSave
 - Download the config file.
 - Augment the current system configuration with the commands in this file.
 - Save the resulting configuration to the file ‘default-save-filename’.
 - Current configuration is saved.

Possible values for the `operation` attribute:

- upgrade
 - Download package.
 - Continue only if serviceAffecting=“yes”

If serviceAffecting=“yes”, execute the following operations:

- Install image (copy image to flash).
 - Switch banks.
 - Reboot
- install
 - Download package.
 - Install image (copy image to flash).
 - Switch banks.
- installDeferActivation
 - Download package.
 - Install image (copy image to flash)
- activate
 - Converts the configuration and changes banks, if required.

- This command does not allow you to switch an invalid bank to a package that does not exist on the device.
- Allows you to choose if the action is to be service disrupting.
- Can be canceled by specifying the currently running bank.
- activateAndWait
 - Switch banks

When upgrading software and system configuration with the same command file, use one of the following combinations:

- configFileRule="activate" operation="upgrade"
Installs a new configuration file, installs the new software where applicable, and if serviceAffecting="yes", reboots the device.
- configFileRule="install" operation="install"
This combination installs a new configuration file in flash, installs new software, then stops. To activate the new software, reboot the device.
- configFileRule="install" operation="upgrade"
Installs a new configuration file, installs the new software, and if serviceAffecting="yes", reboots the device.
- configFileRule="augmentAndSave" operation="upgrade"
Augments the configuration, saves it, upgrades the software, and if serviceAffecting="yes", reboots the device.

The ftpConfigFile parameter can be used to configure the default xFTP setting as specified in a separate xFTP configuration file stored on the xFTP server. This file is automatically created in the switch's file system upon configuring the desired xFTP server and saving the configuration. You can transfer the file to the xFTP server with a name matching the ftpConfigFile parameter in the command file.

For example:

```
system xftp putfile local-filename /mnt/sysfs/system/xFtpConfig remote-filename ciena/
defaultFtpConfig default-server
```

Edit the command file to include the ftpConfigFile parameter:

```
ftpConfigFile="ciena/defaultFtpConfig"
```

Software license fundamentals

A license is a permit to use a premium feature. A license is considered installed or uninstalled based on the presence of one or more license keys. The system software comes with the Base-Features license and supports premium features that require an additional installed license key. A premium feature can consist of a portion of an existing feature, or it can comprise multiple features. Contact your Ciena Sales Rep to obtain advanced feature licensing.

A license key is a data object generated by the Ciena license administrator and installed by an operator. License keys are encrypted and contain no human readable information.

A license key is intended to be used in a specific module within a specific chassis. Note the following:

- On a single module device, the module number is 1.

A license key structure or domain is tied to the switch type. License keys are switch type license keys. For example, a license key structure or domain could be defined to contain all devices in a specific building, or all devices owned by a particular customer, or even a single physical device.

When displaying the status of licenses, a premium feature license shows one of the statuses described in [Table 3-1](#).

Table 3-1
Status of premium feature licenses

Status	Description
Not Installed	Also referred to as an invalid license. None of the operationally-enabled modules has a key installed for this license.
Installed	Also referred to as a valid license. All of the operationally-enabled modules have a key installed for this license and all conditional requirements for the license installation have been satisfied. Conditional requirement are described separately.
Partial License	One or more, but not all, operationally-enabled modules have a key installed for this license.

Note: On devices with option modules, if a premium feature license is installed on module 1 (either implied or specified), but not on modules 2 and 3, events are generated every 60 minutes until the licenses are installed on all modules.

You can install multiple licenses on a device. The names of the licenses and the devices on which they are supported are summarized in [Table 3-2](#).

Table 3-2
License Key Summary

Product	Advanced-10G	Advanced-Ethernet	Advanced-OAM	Advanced-Security	Advanced-Sync	MPLS
3903		x	x	x		
3903x		x	x	x		
3904		x	x	x	x	
3905		x	x	x	x	
3906		x	x	x		
3926	x	x	x	x	x	x
3928	x	x	x	x	x	x
3942	x	x	x	x		x
5142	x	x	x	x	x	x
5160		x	x	x	x	x

A detailed list of the software license keys and associated features is shown in [Table 3-3](#).

Table 3-3
Software License Keys and Features

Software License Requirement	Feature Description
Advanced 10G	10 Gigabit Ethernet support on NNI ports with smaller size Small Form-factor Pluggable (SFP+) Available for 3926, 3928, 3942, and 5142 only. If an NNI port speed is set to 10G and the link is up, but the Advanced 10G license is not installed, the system generates a license violation event every day for the first three events, and then every hour for the next 36 events, and then every 15 minutes for subsequent events.
Advanced-Ethernet	Multi-chassis Link Aggregation Groups (MC-LAG) and inter-chassis link (ICL) protocol are supported.
Advanced Ethernet	Connectivity Fault Management-based link aggregation is supported.
Advanced-Ethernet	Broadcast Containment prevents services from being disrupted by broadcast storms on specified ports
Advanced-Ethernet	Configurable L2 Frame Bandwidth Calculation

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-Ethernet	Configurable Metering Burst Size
Advanced-Ethernet	Configurable per-port RED Egress Queuing
Advanced-Ethernet	Layer 2 Virtual Private Networks (VPNs) enables 802.1ad Provider Bridging to configure Ethernet Private Line/LAN (EPL) and Layer 2 Ethernet Virtual Private Line (EVPL) to deploy Q-in-Q E-line, E-LAN, and E-Tree Ethernet Service Types as defined by the Metro Ethernet Forum (MEF).
Advanced-Ethernet	Ethernet Ring Protection (ERP) Switching, as defined by the G.8032 standard, protects the connectivity between network nodes using the Ring Automatic Protection Switching (R-APS) control protocol. Each node is connected to two adjacent nodes by means of a physical port or link aggregation port forming a closed loop. It provides: • Efficient network connectivity and bandwidth 64Kbps to 100GE capacity. • Loop avoidance. • Link failure detection. • Protection and rapid service recovery within 50 milliseconds (ms). • Client and server layer agnostic implementation. • Use of existing IEEE 802.1 (bridging) and IEEE 802.3 (MAC) hardware. • Standardization (ITU-T SG15/Q9 G.8032) to facilitate multi-vendor interoperability. • Translation into Lower Operational Expenditure (OPEX) and Capital Expenditure (CAPEX). • Implementation in place of Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).
Advanced-Ethernet	Layer 2 Control Frame Tunneling (L2CFT) manages processing and forwarding of untagged L2 control frames and transforming of transparent L2 control frames to L2 Protocol Tunneling (PT) frame format.
Advanced-Ethernet	MAC learning (limited to 4000 entries with base feature license)
Advanced-Ethernet	Multicast Services implement Internet Group Management Protocol (IGMP)

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-Ethernet	Port State Mirroring Groups provide link redundancy by associating the link state of one or more source (uplink) ports with one or more downstream (destination) ports on the switch.
Advanced-Ethernet	Rapid Spanning Tree Protocol (RSTP) provides loop-free topology in a bridged network and delivers efficient reconfiguration of the loop-free topology in the event that a link fails. RSTP, formerly defined in IEEE 802.1w and now incorporated in IEEE 802.1D, was developed in order to achieve faster convergence times. In most circumstances, RSTP can converge the network in less than 32 seconds.
Advanced-Ethernet	Multiple Spanning Tree Protocol (MSTP) is a standards based (IEEE 802.1Q-2005) version of creating multiple spanning trees where each VLAN has its own Multiple Spanning Tree Instance (MSTI). MSTP can be implemented in place of RSTP to provide a loop-free topology in bridged networks and delivers efficient convergence of the loop-free topology in the event that a link fails. MSTP inherits its rapid transition mechanism from RSTP to achieve fast convergence times.
Advanced-Ethernet	Statistics

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-Ethernet	Quality of Service (QoS)-mechanisms for managing bandwidth, including: • traffic profiling, which provides ingress traffic classification and metering • non-conforming ARP discard mode • per-port QoS with CIR/EIR per port • per-port-per-VLAN QoS with CIR/EIR per VLAN • ingress CoS Classification 802.1p/.1D • ingress CoS Classification IPP, DSCP, ingress port ID • L2 priority mapping from IP DSCP/TOS • IP DSCP/TOS mapping from L2 priority • traffic profile on port/CVID/CPRI • named traffic profiles • configurable per-port congestion avoidance processing for managing CoS queue traffic when congestion occurs on egress with RED • configurable egress scheduling, which determines the order in for processing physical queues • configurable egress shaping, which controls bandwidth for taking frames out of queues at egress • configurable frame bandwidth calculation, which configures whether to use the inter-frame-gap (IFG) in the calculations for ingress metering and egress shaping
Advanced-Ethernet	VLAN management for VLAN creation, deletion, and translation for compatibility with Enterprise VLAN applications.
Advanced-Ethernet	System timing: • Synchronous Ethernet (SyncE) • External timing interfaces, that is, Building Integrated Timing Supply (BITS) and Global Positioning System (GPS) • Time Division Multiplexing (TDM)
Advanced-Ethernet	Access control
Advanced-Ethernet	IPv4 DSCP ACLs for Management Traffic
Advanced-Ethernet	Virtual Link Loss Indicator (VLLI)

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-OAM	IEEE 802.3ah Ethernet in the First Mile 802.3ah Operations, Administration and Maintenance (EOAM) provides mechanisms for monitoring point-to-point Ethernet link remote fault indication and remote loopback control. One of the key functions that can be implemented using OAM is remote loopback mode which is a mechanism by which a Data Terminating Equipment (DTE) requests a remote DTE to go into loopback mode. In this mode all frames sent to the remote DTE are looped back unchanged. The return frames can then be analyzed by the sender to determine link quality. Includes loopback and linktrace for troubleshooting and performance measurement.
Advanced-OAM	Connectivity Fault Management (CFM) provides a method to continuously monitor the end-to-end network connectivity of a network service, such as a virtual switch or a VLAN. Services can be monitored over a single hop, a point-to-point link, or over multiple hops, using equipment managed by one or more service providers and operations entities.
Advanced-OAM	IP static routing
Advanced-OAM	NTP Hardware Timestamping maintains accuracy between server updates, tracks time offset and drift, and updates the hardware Real Time Clock (RTC).
Advanced-OAM	RFC 2544 Benchmark Performance Tests Internet Engineering Task Force (IETF)'s RFC 2544 Benchmarking Methodology for Network Interconnect Devices supports the ability to evaluate the performance of network devices.
Advanced-OAM	Two-Way Active Measurement Protocol (TWAMP) provides bi-directional measurements of IP performance between two devices through an exchange of test messages. The system software supports the following TWAMP modes: • TWAMP Light Responder • TWAMP Complete Server • TWAMP Client
Advanced-OAM	Hardware-assisted TWAMP

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-OAM	ITU-T Y.1731 Performance Measurements, introduced by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) complements the IEEE 802.1ag standard, provides the following: • Frame delay - the Delay Measurement Message (DMM) and the Delay Measurement Reply (DMR) include time stamps that are used to calculate two-way frame delay. These measurements are configured per CFM service. Each MEP can be enabled to perform frame delay and frame delay variation measurements between two point-to-point MEPs in the same MA. • Jitter - frame delay variation is calculated by tracking the round-trip DMMs. Note that all DMMs expected must be returned in order to make the jitter calculation. • Frame loss - frame loss is calculated by sending counters within Loss Measurement Messages (LMMs) and Loss Measurement Replies (LMRs). The far-end counters are then compared with the local counters to calculate frame loss for two-way delay measure, port-to-port measurements as a ratio. A bidirectional service is determined unavailable if either of the two directions is declared unavailable; therefore, each MEP must be able to perform near-end and far-end frame loss measurements. • Synthetic frame loss measurement (SLM)- frame loss is calculated using synthetic frames, rather than data traffic. A number of synthetic frames are sent and received, and the system calculates the number of synthetic frames that are lost. This calculation can be treated as a statistical sample, and used to approximate the frame loss ratio of data traffic.
Advanced-Security	The IEEE 802.1x standard defines an authentication protocol that uses a centralized authentication server (typically a RADIUS server) to provide port-based and user-based network access control. This provides a method for authenticating customer premise equipment (CPE) and the Service Delivery Switches and Service Aggregation Switches used to provide the CPE network connection. When a device configured for 802.1x authentication is connected to the network, it passes an authentication request to the device providing its uplink. That device then passes the request through the network to the authentication server, which compares the device's user name and password to a pre-entered subscriber database entry and decides whether to allow the device full access to the network.

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-Security	Remote Authentication Dial-In User Service (RADIUS) is a client/server system used to secure networks against unauthorized remote access. When authenticating a user, the device sends authentication requests to a RADIUS server or servers. The RADIUS servers keep track of all user authentication and service access information. The RADIUS server returns authentication results to the device and the user is either allowed or denied access based on this information. RADIUS servers are also used as the preferred server for 802.1x authentication. The 802.1x framework uses RADIUS messages for communication between the authenticator and the authentication server. For this purpose, RADIUS configuration includes a parameter that allows the RADIUS sever to be designated strictly as a user authentication server, an 802.1x authentication server, or both.
Advanced-Security	The IEEE 802.1x standard defines an accounting protocol that uses a RADIUS server to record what a authorized user is doing. The remote user's accounting information is sent to a designated RADIUS accounting server through accounting requests. This server is typically different from the server used for authentication requests.
Advanced-Security	SSHv2/SFTP - Secure Shell (SSH) provides remote login and Secure FTP (SFTP) file transfers.
Advanced-Security	SNMPv3 encryption and authentication.
Advanced-Security	Terminal Access Controller Access Control System (TACACS)+ is a security protocol that performs the following functions between a Network Access Server (NAS) and an authentication server: • Authentication- Grants users access when they first log in to a device or request a service. • Authorization- Determines which actions users are allowed to perform when they do have access to a device. Authorization will be performed only if authentication was done by TACACS+. • Accounting- Records user actions in order to perform security audits or for billing purposes. Accounting will be performed only if authentication was done by TACACS+.
Advanced-Sync	Advanced packet timing features based on IEEE 1588 version 2 Precision Time Protocol (PTP), including Ordinary Clock (OC) slave clock recovery and Boundary Clock (BC). Available for 3904, 3905, 3926, 3928, 5142 and 5160.
Base-Features	Base Network Time Protocol (NTP)

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Base-Features	Domain Name Services (DNS)
Base-Features	Dying Gasp trap
Base-Features	Dynamic Host Control Protocol (DHCP) client
Base-Features	Eight Class of Service Queues with Default CoS Mapping
Base-Features	External timing interface support
Base-Features	File Transfer Protocol (FTP)
Base-Features	IP Access Control Lists (IP-ACLs)
Base-Features	Line Rate Switching
Base-Features	MAC Learning up to 4000 entries
Base-Features	Management VLANs 1 and 127
Base-Features	Port Management
Base-Features	Remote Monitoring (RMON)
Base-Features	Simple Network Management Protocol (SNMP) v1/v2c
Base-Features	Strict Priority Scheduling

Table 3-3
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Base-Features	Trivial File Transfer Protocol (TFTP)
Base-Features	802.1AX Link Aggregation Control Protocol (LACP) as defined in IEEE 802.1AX combines two or more full-duplex Ethernet ports of the same speed into a single logical port to carry traffic between two devices connected in parallel. LACP enables load sharing, load balancing, bandwidth expansion, and link redundancy.
MPLS	Multi-Protocol Label Switching (MPLS) for creation of Layer 2 (L2) Virtual Private Networks (VPNs) and associated protocols, including: • Label Distribution Protocol (LDP). • Open Shortest Path First (OSPF). • Open Systems Interconnect (OSI) Intermediate System to Intermediate System (IS-IS) Intra-domain Routing Protocol. • ReSerVation Protocol with Traffic Engineering (RSVP-TE). • Alarm Indication Signal with Link Down Indication (AIS/LDI) • Bidirectional Forwarding Detection (BFD) • VPLS Integrated Routing and Bridging • Border Gateway Protocol (BGP)

Managing system software

This chapter provides the following procedures:

- “Specifying xFTP server settings” on page 4-3
- “Transferring files” on page 4-7
- “Upgrading using the CLI and a command file” on page 4-9
- “Upgrading using the CLI without a command file” on page 4-12
- “Upgrading using a DHCP server” on page 4-16
- “Upgrading using the software install command” on page 4-18
- “Activating the software” on page 4-26
- “Generating sequence reports” on page 4-27
- “Backing up software images” on page 4-30
- “Displaying board support and datapath FPGA version information” on page 4-31

Note 1: The procedures in this chapter assume you are upgrading from 6.9.0 or higher.

Note 2: After upgrading SAOS, configuration changes are made that may not be backwards compatible. If a downgrade occurs, such changes can cause configuration errors after a reboot. To avoid configuration errors for a planned downgrade, do not save the configuration. Otherwise, save the configuration after the upgrade.

Note 3: If the package-path parameter is left unspecified, packages must be located in the <xftpoot>/ciena/packages/saos-<build> directory on the xFTP server or the upgrade will fail.

Types of resets

There are two types of resets: warm-start (default) and cold-start. A warm-start reset is a control plane reset of the CPU, RAM, NOR flash and NAND flash. POST is not executed and the dataplane is preserved for the major portion of the reboot cycle of the node. A cold-start reset is a control and data plane reset. The Broadcom switch, the CPU, RAM, NOR flash and NAND flash are reset. A cold-start reset occurs only if the user specifies the “cold-

start” option along with the “chassis reboot” or “software upgrade” commands during a reboot or software upgrade. The Push button reset always triggers a cold start.

System initialization changes ensure that control over the resets for all data plane devices is delegated to the SAOS application and early system initialization does not touch those reset lines. Loading of the configuration files varies depending on the size of the configuration files.

Note: Warm-start can be performed only when upgrading from SAOS 6.12 or later.

Procedure 4-1

Specifying xFTP server settings

Various system processes transfer files from an external xFTP server, including software upgrades or downgrades and augmenting or installing configuration files. [Table 4-1](#) lists the attributes for specifying the xFTP server.

Table 4-1
xFTP Server Settings

Designated xFTP server attribute(s)	Description
server-port <INTEGER: 1..65535>	Server port number for the TFTP/FTP/SFTP server
ftp-server <ip-host-str>	FTP server specified by IP address or host name (if DNS is configured).
tftp-server <ip-host-str>	TFTP server specified by IP address or host name (if DNS is configured).
sftp-server <ip-host-str>	SFTP server specified by IP address or host name (if DNS is configured).
login-id <username>	TFTP/FTP/SFTP username.
password-attr	Enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
mode <tftp ftp sftp>	Sets the xFTP mode, FTP, SFTP, or TFTP. Default is TFTP.
server <IpHost>	Sets the xFTP server by IP address or host name using the default server mode.
connection-timeout <NUMBER: 1-100>	Time to wait (in seconds) before the retry times out. Default is 5 seconds.
retries <NUMBER: 1-10>	Maximum number of retries. Default is 2.
retry-interval <NUMBER: 1-300>	Time to wait (in seconds) between retries. Default is 15.
url <String>	The remote file URL.
cold-start	Optional command that performs a cold-start reset of the control and data plane. The default is warm-start reset.
service-disruption <allow deny>	Service disruption permission.
defer-activation	Defers the software installation so that it will not boot this bank upon the next reboot.

Software management commands that transfer files (such as, upgrade, install, and run), provide attributes to override the configured xFTP server IP host, login-id and echoless password settings listed in [Table 4-1](#). The software upgrade command can also override the connection-timeout, retries, and retry-interval settings. Optionally, these software management commands can be run to select one of the default servers as listed in [Table 4-2](#).

Table 4-2
Default xFTP server selection

Default xFTP server selection	Description
default-tftp-server	Specifies the default TFTP server if configured by the “system xftp set tftp-server <IpHost>” command.
default-ftp-server	Specifies the default FTP server if configured by the system xftp set ftp-server <IpHost>” command.
default-server	Specifies the default xFTP server if configured by the system xftp set ftp-server <IpHost>” and “system xftp set mode” command. Supported for backward compatibility.
default-sftp-server	Specifies the default SFTP server as configured by the “system xftp set sftp-server <IpHost>” command.

Step	Action
------	--------

To configure the xFTP server and settings

- 1 Configure the TFTP, FTP, and SFTP server:

```
system xtftp set {tftp-server <ip-host-str> [login-id  
<username> [<password-attr>|<echoless-password-attr>]  
[server-port <INTEGER: 1..65535>]]}  
  
system xftp set {ftp-server <ip-host-str> [login-id  
<username> [<password-attr>|<echoless-password-attr>]  
[server-port <INTEGER: 1..65535>]]}
```

where

tftp-server <IP address or host name>	is the tftp server name.
login-id <username>	is the TFTP username.
password-attr	enters the password in clear text.
echoless- password-attr	engages an echoless password collector.

where

server-port is the server-port number.

<INTEGER:

1..65535>

ftp-server <ip- is the ftp server name.
host-str>

login-id is the FTP username.
<username>

- 2 Configure the xFTP retries retry-interval, connection-timeout, and mode settings:

```
system xftp set retries <NUMBER: 1-10> retry-interval
<NUMBER: 1-300> connection-timeout <NUMBER: 1-100> mode
<tftp|ftp|sftp>
```

To restore xFTP server settings to default

- 3 If you want to restore xFTP server settings to the default, clear the server settings and set the mode to TFTP:

```
system xftp unset tftp-server
system xftp unset ftp-server
system xftp unset sftp-server
system xftp set mode tftp
```

To confirm and save the configuration

- 4 Confirm the configuration:

```
system xftp show
```

- 5 Save the configuration:

```
configuration save
```

The xFTP settings are saved in the configuration file as well as in a separate file called xFtpConfig in the /mnt/sysfs/system/ directory of the file system. These files are persistent upon reboot and upgrade.

—end—

Example

This example configures TFTP server settings and sets the default mode to TFTP.

```
system xftp set ftp-server 192.0.2.0 login-id myFTPUser
echoless-password
system xftp set sftp-server 198.51.100.0 login-id
mySFTPUser echoless-password
system xftp set tftp-server 203.0.113.0
system xftp set mode tftp
system xftp show
```

+-----+----- XFTP SETTINGS -----+

4-6 Managing system software

Default Mode	TFTP
Tftp Host (User)	203.0.113.0
Tftp Host (DHCP)	
Tftp Host (Oper)	203.0.113.0
Tftp Client State	Enabled
Ftp Host Name	192.0.2.0
Ftp Login ID	myFTPuser
Ftp Client State	Enabled
Sftp Host Name	
Sftp Login ID	
Connection Timeout (Sec)	15
Retry Interval (Sec)	15
Retries	2

Procedure 4-2

Transferring files

General system commands for transferring files support the use of the xFTP server selection.

Step	Action
------	--------

To transfer files to an xFTP server

- Transfer files to an xFTP server:

```
system xftp putfile {local-filename <String>
{remote-filename <String>}
{default-server|default-ftp-server|default-tftpserver|
default-sftp-server|
{tftp-server <ip-host-str> [server-port <INTEGER:
1..65535>]}
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echolesspassword-attr>][server-port
<INTEGER: 1..65535>]}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echolesspassword-attr>}[server-port
<INTEGER: 1..65535>}}}[url <String>
]
```

where

local-filename <String>	is the local filename.
remote-filename <String>	is the remote filename.
default-server	uses the default xFTP server.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-sftp-server	uses the default SFTP server.
tftp-server <IP-host-str>	is the TFTP server.
server-port <INTEGER: 1..65535>	is the server port number.
ftp-server <IP-host-str>	is the FTP server name.

where

login-id	is the TFTP/FTP/SFTP username.
<username>	
password-attr	enters the password in clear text.
echoless- password-attr	engages an echoless password collector.
sftp-server <IP- host-str>	is the SFTP server.
url <String>	is the remote file URL.

To receive files from an xFTP server

2 Receive files from an xFTP server:

```
system xftp getfile {local-filename <String>
{remotefilename <String>}
{default-server|default-ftp-server|default-tftpserver|
default-sftp-server|
{tftp-server <ip-host-str> [server-port <INTEGER:
1..65535>]}}
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echolesspassword-attr>][server-port
<INTEGER: 1..65535>]}}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echolesspassword-attr>}[server-port
<INTEGER: 1..65535>]}}
[url <String>
```

—end—

Example

The following example transfers files to an xFTP server.

```
system xftp putfile default-sftp-server local-filename config/
startup-config remote-filename test-test-test
```

The following example receives files from an xFTP server.

```
system xftp getfile default-sftp-server remote-filename test-
test-test local-filename config/startup-config
```

Procedure 4-3

Upgrading using the CLI and a command file

The following commands can be run using any user account with a privilege level of super-user.

Step	Action
1	Ensure that the device has network connectivity to the xFTP server. <pre>ping <IP Address or Host Name></pre> where IP Address or Host Name is the IP address or host name of the xFTP server.
2	Save the configuration. <pre>configuration save</pre>
3	Run the command file, specifying the desired directory, command file, and xFTP server attribute(s). <pre>software run {command-file <String>} [server <IP address or host name>] {default-server default-ftp-server default-tftpserver default-sftp-server tftp-server <ip-host-str> [server-port <INTEGER: 1..65535>]} {ftp-server <ip-host-str> [login-id <username> [<password-attr> <echolesspassword-attr>] [server-port <INTEGER: 1..65535>]] {sftp-server <ip-host-str> login-id <username> {<password-attr> <echolesspassword-attr>} [server-port <INTEGER: 1..65535>]]}</pre> where command-file <String> is the filename of the command file including path. default-server uses the default xFTP server. default-tftp-server uses the default TFTP server. default-ftp-server uses the default FTP server. default-sftp-server uses the default SFTP server. tftp-server <IP address or host name> is the TFTP server.

where

login-id is the TFTP/FTP/SFTP username.
<username>

password-attr enters the password in clear text.

echoless- engages an echoless password collector.
password-attr

sftp-server <IP- is the SFTP server.
host-string>

Note 1: The upgrade process begins immediately and can take up to 10 minutes to complete.

Note 2: If you specify only the path (the path name must end with a slash to distinguish it from a file name) of the command file, the device searches the directory for the most specific command file in the following order.

- a. Device specific file named with its MAC address.
- b. Switch class file for its switch, artimir.xml or brego.xml
- c. Generic switch class file, le-lnx.xml

Once the most specific command file has been selected, the device runs the section of the command file with the most specific switch class. So, if the command file has an artimir section and an le-lnx section, the device will process the artimir section, and skip the le-lnx section.

Note 3: The command file name needs to be different for the host to download it. If the switch is provided with the same command file name that has been previously used it will not download it again.

- 4 Confirm that the software is installed.

software show

—end—

Example

The following example runs the le-lnx.xml command file to upgrade using the default server.

```
> ping 192.0.2.0
PING 192.0.2.0 (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: seq=0 ttl=62 time=0.428 ms
64 bytes from 192.0.2.0: seq=1 ttl=62 time=0.328 ms
64 bytes from 192.0.2.0: seq=2 ttl=62 time=0.337 ms

--- 192.0.2.0 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.328/0.364/0.428 ms
DEN-Lab-3942-34*> software run command-file /ciena/packages/saos-06-16-01-0182/le-lnx.xml default-ftp-server
NOTE: This operation cannot be interrupted once it has started.
WORKING: downloading file remote /ciena/packages/saos-06-16-01-0182/le-lnx.xml local /tmp/command.xml
WORKING: FTP file download in progress
```

```

WORKING: downloading file remote ciena/packages/saos-06-16-01-0182/pmf-saos-
06-16-01-0182.xml local /mnt/sysfs/software/pmf-saos-06-16-01-0182.xml
WORKING: FTP file download in progress
WORKING: downloading file remote ciena/packages/saos-06-16-01-0182/le-
14596.chk local /tmp/xgrade/images/le-14596.chk
WORKING: FTP file download in progress
WORKING: running check script le-14596.chk on file /tmp/xgrade/images/le-
14596.chk
WORKING: file check ok
WORKING: downloading file remote ciena/packages/saos-06-16-01-0182/le-
14596.cavium.ins local /tmp/xgrade/images/le-14596.cavium.ins
WORKING: FTP file download in progress
WORKING: running check script le-14596.chk on file /tmp/xgrade/images/le-
14596.cavium.ins
WORKING: file check ok
WORKING: Installing Image le-14596.cavium.ins
WORKING: install script /tmp/xgrade/images/le-14596.cavium.ins will be used
WORKING: downloading file remote ciena/packages/saos-06-16-01-0182/le-
14596.caliondo_nand.tar.xz local /tmp/xgrade/images/le-
14596.caliondo_nand.tar.xz
WORKING: FTP file download in progress
WORKING: running check script le-14596.chk on file /tmp/xgrade/images/le-
14596.caliondo_nand.tar.xz
WORKING: file check ok
WORKING: Installing Image le-14596.caliondo_nand.tar.xz

```

Connection to host lost.

DEN-Lab-3942-34> software show

Installed Package	: saos-06-16-01-0182
Running Package	: saos-06-16-01-0182
Application Build	: 14596
Package Build Info	: Tue Jul 18 18:05:08 2017 autouser onxvpnj04
Running Kernel	: 3.10.54-grsec
Running MIB Version	: 04-16-01-0047
Release Status	: GA
Running bank	: A
Bank package version:	saos-06-16-01-0182
Bootloader version	: 14596
Bootloader status	: valid
Bank status	: not validated
Standby bank	: B
Bank package version:	saos-06-16-01-0172
Bootloader version	: 14508
Bootloader status	: valid
Bank status	: valid
Last command file:	/ciena/packages/saos-06-16-01-0182/le-lnx.xml
Last configuration file:	unknown

DEN-Lab-3942-34>

Procedure 4-4

Upgrading using the CLI without a command file

The following commands can be run using any user account with a privilege level of super-user.

**CAUTION****Automatic Reboot of the System**

The upgrade process described in this section causes the system to reboot automatically.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Ensure that the device has network connectivity to the xFTP server. |
|---|---|

`ping <IP Address or Host Name>`

where

IP Address or Host Name is the IP address or host name of the xFTP server.

- | | |
|---|-------------------------|
| 2 | Save the configuration. |
|---|-------------------------|

`configuration save`

3 Upgrade the system software and reboot automatically specifying the desired software package and xFTP server attribute(s).

```
software upgrade {package <String>} [package-path
<String>] [server <IP address or host name>] [ipv6-server
<String>] [retries <NUMBER: 1..10>] [retry-interval
<SECONDS: 1..300>] [cold-start] [connection-timeout
<SECONDS: 1..100>] [service-disruption <allow|deny>]
{default-server|default-ftp-server|default-tftpserver|
default-sftp-server|
{tftp-server <ip-host-str> [server-port <INTEGER:
1..65535>]]}
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echolesspassword-attr>] [server-port
<INTEGER: 1..65535>]]|
{sftp-server <ip-host-str> login-id <username> {<password-
attr>|<echolesspassword-attr>} [server-port <INTEGER:
1..65535>]]}}
```

where

package-file <String>	is the software package path.
package-path <String>	is the full path to the package directory.
server <IP address or host name>	is the FTP server.
ipv6-server <String>	is the IPv6 xFTP server.
retries <NUMBER: 1..10>	is the number of retries. Valid values are numbers from 1 to 10.
retry-interval <SECONDS: 1..300>	is the retry interval. Valid values are numbers from 1 to 300.
connection- timeout <SECONDS: 1..100>	is the connection-timeout. Valid values are numbers from 1-100.
cold-start	optional command that performs a cold-start reset of the control and data plane. The default is warm-start reset.
service- disruption <allow deny>	is the service disruption permission.
default-server	uses the default xFTP server.

where

default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-sftp-server	uses the default SFTP server.
tftp-server <IP-host-str>	is the TFTP server.
server-port <INTEGER: 1..65535>	is the server port number.
ftp-server <IP-host-str>	is the FTP server name.
login-id <username>	is the TFTP/FTP/SFTP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
sftp-server <IP-host-str>	is the SFTP server.

Note: The upgrade process may take up to 10 minutes to complete.

—end—

Example

The following example upgrades without a command file using the default server. This example shows the option of a cold-start reset.

```
> ping 192.0.2.0
PING 192.0.2.0 (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: seq=0 ttl=62 time=0.428 ms
64 bytes from 192.0.2.0: seq=1 ttl=62 time=0.328 ms
64 bytes from 192.0.2.0: seq=2 ttl=62 time=0.337 ms

--- 192.0.2.0 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.328/0.364/0.428 ms
> software upgrade package saos-<build> default-server service-disruption
allow cold-start
NOTE: This operation cannot be interrupted once it has started.
WORKING: downloading file remote /ciena/packages/saos-<build>/le-lnx.xml
local /tmp/command.xml
WORKING: tftp file download in progress
WORKING: downloading file remote ciena/packages/saos-<build>/pmf-saos-
<build>.xml local /mnt/sysfs/software/pmf-saos-<build>.xml
WORKING: tftp file download in progress
WORKING: downloading file remote ciena/packages/saos-saos-<build>/le-8506.chk
local /tmp/xgrade/images/le-8506.chk
WORKING: tftp file download in progress
```

```

WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-
8506.chk
WORKING: file check ok
WORKING: downloading file remote ciena/packages/saos-<build>/le-8506-
cavium.ins local /tmp/xgrade/images/le-8506-cavium.ins
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
cavium.ins
WORKING: file check ok
WORKING: Installing Image le-8506-cavium.ins
WORKING: install script /tmp/xgrade/images/le-8506-cavium.ins will be used
WORKING: downloading file remote ciena/packages/saos-<build>/le-8506-
3942.tar.xz local /tmp/xgrade/images/le-8506-
3942.tar.xz
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
3942.tar.xz
WORKING: file check ok
WORKING: Installing Image le-8506-3942.tar.xz

```

Connection to host lost.

> software show

```

+-----+
| Installed Package      : saos-<build>
| Running Package       : saos-<build>
| Application Build      : 8506
| Package Build Info    : Mon Nov 11 01:08:04 2013 autouser wax-centaur-12
| Running Kernel        : 2.6.35.10
| Running MIB Version   : 04-10-00-0060
| Release Status        : Beta
+-----+
| Running bank          : B
| Bank package version:  : saos-<build>
| Bootloader version   : 8506
| Bootloader status    : valid
| Bank status          : valid (validated      0hr 15min 36sec ago)
| Standby bank         : A
| Bank package version:  : saos-<build>
| Bootloader version   : 8432
| Bootloader status    : valid
| Bank status          : valid (validated      0hr 15min 14sec ago)
+-----+
| Last command file:    /ciena/packages/saos-<build>/le-lnx.xml
| Last configuration file: unknown
+-----+

```

Procedure 4-5

Upgrading using a DHCP server

This method of upgrade uses a DHCP server to trigger the upgrade process through the use of a command file.

Use the DHCP option 'bootfile' specify the command file. A fully qualified filename (path1/path2/file.xml) can be used or a directory name such as "path1/path2/" can be specified. Path names must end with a slash to distinguish them from a file name, for example:

- bootfile = "ciena/packages/saos-06-13-00-0222/"
- bootfile = "ciena/packages/saos-06-13-00-0222/command-saos-06-13-00-0222.xml"
- bootfile = "cmd/my-command-file.xml"

If you specify a directory as the bootfile, the device tries to download the file MAC.xml where MAC is the Ethernet MAC address of the device (for example, 0002a1010203.xml). If that fails, the device tries to download the file le-lnx.xml.

Note: When a configuration file is processed due to a request from DHCP, the device saves the filename (last-config-file) and it does not process the same file name twice. You need to reset this file name in order to process the same configuration file a second time. The same is true for the command file name as well.

Step	Action						
1	Configure the DHCP server: <table border="1"> <thead> <tr> <th>If you are using a</th><th>Then</th></tr> </thead> <tbody> <tr> <td>DHCPv4 server</td><td> Configure • Next Server (option 66): Specifies the IP address of the TFTP server. • Boot File (option 67): Specifies the path to the command file directory or the full path to the command file itself. </td></tr> <tr> <td>DHCPv6 server</td><td> Configure boot-file-url (option 59), which specifies the URL to the boot file (by means of tftp only, for example, tftp://myserver/bootfile). </td></tr> </tbody> </table>	If you are using a	Then	DHCPv4 server	Configure • Next Server (option 66): Specifies the IP address of the TFTP server. • Boot File (option 67): Specifies the path to the command file directory or the full path to the command file itself.	DHCPv6 server	Configure boot-file-url (option 59), which specifies the URL to the boot file (by means of tftp only, for example, tftp://myserver/bootfile).
If you are using a	Then						
DHCPv4 server	Configure • Next Server (option 66): Specifies the IP address of the TFTP server. • Boot File (option 67): Specifies the path to the command file directory or the full path to the command file itself.						
DHCPv6 server	Configure boot-file-url (option 59), which specifies the URL to the boot file (by means of tftp only, for example, tftp://myserver/bootfile).						
2	Enable the DHCP client on the device. <pre>dhcp client enable</pre>						

3 Save the configuration.

`configuration save`

The upgrade process begins as soon as a DHCP renew occurs and may take up to 10 minutes to complete.

—end—

Procedure 4-6

Upgrading using the software install command

Use the software install command to download and install software into flash memory immediately, and when a reboot is requested the device will then boot using the new software. Note that once the operation has started, it cannot be interrupted. A series of messages are displayed to indicate the status of the installation.

Step	Action
1	Ensure that the device has network connectivity to the xFTP server: <pre>ping <IP Address or Host Name></pre> where IP Address or Host Name is the IP address or host name of the xFTP server.
2	Save the configuration: <pre>configuration save</pre>
3	Install the new software package into flash: <pre>software install {package <String>} [package-path <String>] [server <IP address or host name> [defer- activation] {default-server default-ftp-server default-tftpserver default-sftp-server {tftp-server <ip-host-str> [server-port <INTEGER: 1..65535>]]} {ftp-server <ip-host-str> [login-id <username> [<password-attr> <echoless-password-attr>] [server-port <INTEGER: 1..65535>]]} {sftp-server <ip-host-str> login-id <username> {<password-attr> <echoless-password-attr>] [server-port <INTEGER: 1..65535>]]}}</pre> where package <String> is the software package path. Supported on switches with two flash banks. package-path <String> is the full path to the package directory. server <IP address or host name> is the TFTP server. Supported on switches with two flash banks.

where

`defer-activation` defers the software installation so that it will not boot this bank upon the next reboot.

`default-server` uses the default xFTP server.

`default-ftp-server` uses the default FTP server.

`default-tftp-server` uses the default TFTP server.

`default-sftp-server` uses the default SFTP server.

`tftp-server <IP-host-str>` is the TFTP server.

`server-port <INTEGER: 1..65535>` is the server port number.

`ftp-server <IP-host-str>` is the FTP server name.

`login-id <username>` is the TFTP/FTP/SFTP username.

`password-attr` enters the password in clear text.

`echoless-password-attr` engages an echoless password collector.

`sftp-server <IP address or host name>` is the SFTP server.

4 Validate the software:

```
software validate
```

5 Reboot the chassis so the new package is now the running package:

```
chassis reboot now cold-start
```

Note: Adding the optional cold-start command if you want to take down the data plane while upgrading. If you do not wish to perform a cold-start reset, omit this option. The default is warm-start.

6 Confirm the Installed Package and Running Package:

```
software show
```

—end—

Example

This example installs software using the default server.

```
> ping 192.0.2.0
PING 192.0.2.0 (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: seq=0 ttl=62 time=0.428 ms
64 bytes from 192.0.2.0: seq=1 ttl=62 time=0.328 ms
64 bytes from 192.0.2.0: seq=2 ttl=62 time=0.337 ms
--- 192.0.2.0 ping statistics ---
```

4-20 Managing system software

```
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.328/0.364/0.428 ms
> configuration save
> software install package saos-<build> default-server
NOTE: This operation cannot be interrupted once it has started.
WORKING: downloading file remote ciena/packages/saos-<build>/pmf-saos-
<build>.xml local /mnt/sysfs/software/pmf-saos-<build>.xml
WORKING: tftp file download in progress
WORKING: downloading file remote ciena/packages/saos-<build>/le-8506.chk
local /tmp/xgrade/images/le-8506.chk
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-
8506.chk
WORKING: file check ok
WORKING: downloading file remote ciena/packages/saos-<build>/le-8506-
cavium.ins local /tmp/xgrade/images/le-8506-cavium.ins
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
cavium.ins
WORKING: file check ok
WORKING: Installing Image le-8506-cavium.ins
WORKING: install script /tmp/xgrade/images/le-8506-cavium.ins will be used
WORKING: downloading file remote ciena/packages/saos-<build>/le-8506-
3942.tar.xz local /tmp/xgrade/images/le-8506-3942.tar.xz
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
3942.tar.xz
WORKING: file check ok
WORKING: Installing Image le-8506-3942.tar.xz
> chassis reboot now
proceeding to reboot
>
```

Connection to host lost.

```
> software show
```

Installed Package	: saos-<build>
Running Package	: saos-<build>
Application Build	: 8506
Package Build Info	: Mon Nov 11 01:08:04 2013 autouser wax-centaur-12
Running Kernel	: 2.6.35.10
Running MIB Version	: 04-10-00-0060
Release Status	: Beta

Running bank	: B
Bank package version:	saos-<build>
Bootloader version	: 8506
Bootloader status	: valid
Bank status	: valid (validated 0hr 15min 36sec ago)
Standby bank	: A
Bank package version:	saos-<build>
Bootloader version	: 8432
Bootloader status	: valid
Bank status	: valid (validated 0hr 15min 14sec ago)

Last command file: /ciena/packages/saos-<build>/le-lnx.xml	
Last configuration file: unknown	

Procedure 4-7

Upgrading the SFP packet processor

An alarm is raised when a newer version of the SFP packet processor is available than the one running on the SFP. The SFP packet processor upgrade is not part of the standard SAOS upgrade process as it takes over 5 minutes to complete and the data path to the transceiver must be set up. The SAOS load contains the image for the SFP packet process upgrade meaning no extra file transfer is required.

The SFP packet processor has an active bank and a standby bank. The upgrade procedure upgrades the standby bank and once the upgrade is successful, the banks are swapped. During this time, there is a service disruption.

During the SFP packet processor upgrade process, an info alarm is raised in increments of 10 percent successful completion as a heartbeat. If the upgrade is not successful, an alarm is raised. When the upgrade is successfully completed, an info alarm is raised to inform of the completing of the upgrade. Only one SFP may be upgraded or downgraded at a time. The TDM SFP must be configured and enabled to upgrade it.

Bulk upgrades is useful on devices with many SFPs inserted. The bulk command can be run when an individual SFP is not being upgraded or the bulk command is not already running. When a bulk upgrade is running, individual SFPs cannot be upgraded.

The command specifies a list of SFPs to upgrade and each SFP is upgraded one after the other. The command starts at the first port specified and continues until it reaches the last port specified. Any SFP in the list that is not a TDM SFP is ignored. If an SFP upgrade fails, the command moves to the next SFP. If an SFP is inserted into a port that has already been checked, it will not be upgraded as part of the command.

An SFP is upgraded if it is inserted into a port that has not yet been checked. Removing a SFP that is being upgraded moves the upgrade to the next SFP after a time-out period. The bulk upgrade can be requested to stop, but it must first complete the current SFP being upgraded.

You can view the status of the bulk upgrade.

Step	Action
------	--------

- 1 Upgrade the packet processor in the TDM SFP:

```
software upgrade port <port-list> [now|stop]
```

where

port <port-list> is the port(s) to upgrade.

now|stop starts or stops the upgrade immediately.

- 2 Display the active and standby version of the software on the TDM SFP and the packet processor version:

```
software show port <port-list>
```

—end—

Example

The following example shows the output for the software show command for port 1-10.

```
> software show port 1-10
```

TDM SFP Ports Bulk Upgrade Status									
TDM Port	Phys Port	Admin State	Available Version	Running Version	Operation Required	Upgrade Result	Load Progress	Bulk Status	
port1	1	enabled	0802000001	0802000001	None	Successful	0%	Up To Date	
port2	2	enabled	08000a0001	08000a0001	None	Successful	0%	Up To Date	
port3	3	enabled	0801000001	0801000001	None	Successful	0%	Up To Date	
port8	8	enabled	0801000001	0700010001	Upgrade	Successful	0%	In Progress	

Procedure 4-8

Downgrading the SFP packet processor

When a switch is downgraded, the packet processor on the SFP may not be compatible with the current software. In this case, the SFP must be downgraded before it can function.

For SFP ports on downgrade, the following attributes are removed:

- Signal-degrade
- Signal-fail
- Mac

Step	Action
------	--------

- | | |
|---|--|
| 1 | Downgrade the packet processor in the TDM SFP: |
|---|--|

```
software upgrade port <port-list> [now]
```

where

port <port-list> is the port(s) to upgrade.

now starts the downgrade immediately.

- | | |
|---|---|
| 2 | Display the active and standby version of the software on the TDP SFP and the packet processor version: |
|---|---|

```
software show port <port-list>
```

—end—

Procedure 4-9

Upgrading the TDM module packet processor

An alarm is raised when a newer version of the TDM module packet processor is available than the one running on the 3926 device. The TDM module packet processor upgrade is not part of the standard SAOS upgrade process as it takes over 5 minutes to complete and the data path to the TDM module must be set up. The SAOS load contains the image for the TDM module upgrade meaning no extra file transfer is required.

The TDM module has an active bank and a standby bank. The upgrade procedure upgrades the standby bank and once the upgrade is successful, the banks are swapped. During this time, there is a service disruption.

During the TDM module packet processor upgrade process, an info alarm is raised in increments of 10 percent successful completion as a heartbeat. If the upgrade is not successful, an alarm is raised with a reason code. When the upgrade is successfully completed, an info alarm is raised to inform of the completing of the upgrade.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Upgrade the packet processor in the TDM module:
<code>software upgrade module [now]</code>
where
<code>now</code> starts the upgrade immediately. |
| 2 | Display the active and standby version of the software on the TDM module and the packet processor version:
<code>software show module</code>
—end— |

Procedure 4-10

Downgrading the TDM module packet processor

When a switch is downgraded, the packet processor on the TDM module may not be compatible with the current software. In this case, the TDM module must be downgraded before it will function.

For SFP ports on downgrade, the following attributes are removed:

- Signal-degrade
- Signal-fail
- Mac

Step	Action
------	--------

- | | |
|---|---|
| 1 | Downgrade the packet processor in the TDM module: |
|---|---|

```
software upgrade module [now]
```

where

now starts the downgrade immediately.

- | | |
|---|--|
| 2 | Display the active and standby version of the software on the TDM module and the packet processor version: |
|---|--|

```
software show module
```

—end—

Procedure 4-11

Activating the software

Activate the software installed in the release directory. You must install the software before using the activate command.

Step	Action
------	--------

- | | |
|---|---|
| 1 | <p>Activate the software installed in the release directory:</p> <pre>software activate [package <package-name>] [service-
disruption <allow deny>] [force-standby]</pre> <p>where</p> <p>package is the package release name.
 <package-name></p> <p>service-
disruption sets the service disruption permission.
 <allow deny></p> <p>[force-standby] forces the activation of the standby software bank.</p> |
|---|---|

—end—

Procedure 4-12

Generating sequence reports

You can generate:

- a report that shows a sequence of actions the software manager would need to do in order to install the desired package. The report includes information about service disruption. This command does not perform any of the actions. This procedure only applies to switches with two flash banks.
- a detailed report that indicates the actions required to process the command file
- a report to outline upgrade requirements

Step	Action
------	--------

To generate a sequence report

- 1 Generate a sequence report:

```
software report-sequence install {package <String>}
[package-path <package path>] [server <IP address or host
name>] [defer-activation]
{default-server|default-ftp-server|default-tftpserver|
default-sftp-server|
{tftp-server <ip-host-str> [server-port <INTEGER:
1..65535>]}
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echoless-password-attr>] [server-port
<INTEGER:1..65535>]}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echoless-password-attr>} [server-port
<INTEGER: 1..65535>}]}}
```

where

package <String> is the software package path.

[package-path <package path>] is the full path to the package directory.

server <IP address or host name> is the TFTP server. Supported on switches with two flash banks.

defer-activation defers the software installation so that it will not boot this bank upon the next reboot.

default-server uses the default xFTP server.

where	
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-sftp-server	uses the default SFTP server.
tftp-server <IP-host-str>	is the TFTP server.
server-port <INTEGER>	is the server port number.
ftp-server <IP-host-str>	is the FTP server name.
login-id <username>	is the TFTP/FTP/SFTP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
sftp-server <IP address or host name>	is the SFTP server.

To generate a detailed report to help process the command file

- 2 Generate a detailed report to indicate the actions required to process the command file:

```
software report-sequence run {command-file <file>}  
{[server <IP address or host name>]}  
{default-server|default-ftp-server|default-tftp-server|  
default-sftp-server|  
{tftp-server <ip-host-str> [server-port <INTEGER:  
1..65535>]}  
  
{ftp-server <ip-host-str> [login-id <username>  
[<password-attr>|<echoless-password-attr>][server-port  
<INTEGER:1..65535>]}|  
  
{sftp-server <ip-host-str> login-id <username>  
{<password-attr>|<echoless-password-attr>}[server-port  
<INTEGER: 1..65535>]}}}
```

where

command-file <file>	is the command file name.
------------------------	---------------------------

To generate a detailed report to outline the upgrade requirements

- 3 Generate a detailed report to indicate the actions required to process the command file:

```
software report-sequence upgrade {package <String>}  
[package-path <package path>] [default-server] [default-  
tftp-server] [default-ftp-server] [default-sftp-server]  
[tftp-server <IP address or host name>] [ftp-server <IP  
address or host name>] [sftp-server <IP address or host  
name>]
```

—end—

Procedure 4-13

Backing up software images

The 3903, 3903x, 3904, 3905, 3906, 3926, 3928, 3942, 5142 and 5160 have two flash image banks instead of a single flash image bank. The second image bank holds a backup copy of the system software. If the primary image bank becomes corrupted, the system automatically switches to the backup bank.

When the software upgrade command is used, the new software is installed in one image bank only. The old software remains in the other image bank. Once the new software is installed and running, you can back up the new software. It is highly recommended (but not required) that you back up the new software after each upgrade.

Step	Action
------	--------

1	Back up the new software image:
---	---------------------------------

	<code>software protect</code>
--	-------------------------------

2	Confirm information for both flash image banks:
---	---

	<code>software show</code>
--	----------------------------

—end—

Procedure 4-14

Displaying board support and datapath FPGA version information

Display board support and datapath field-programmable gate array (FPGA) version information.

Step	Action
1	Display board support and datapath FPGA: <code>software fpga show</code>
2	To display FPGA information for a Combo TDM OC48 FRU module in a 3926, use the following command: <code>software show module</code>
—end—	

Examples

The following example shows the output for the `software fpga show` command on a 3903 device.

```
3903> software fpga show
+-----+ BOARD SUPPORT FPGA +-----+
| Name   | Version |
+-----+-----+
| amroth | 00.0B.0C |
+-----+-----+

+-----+ DATAPATH FPGA +-----+
| Name   | Version | Module |
+-----+-----+-----+
| greylin | 03.05.01 | -      |
+-----+-----+-----+
```

The following example shows the output for the `software show module` command on a 3926 with a Combo TDM OC48 FRU module.

```
3926> software show module
+-----+ COMBO FRU MODULE FPGA +-----+
| FPGA Name | Running Fpga Version | Available Fpga Version |
+-----+-----+-----+
| SARN      | 00.00.11              | 00.00.11              |
| NORBORN   | 01.01.0e              | 01.01.0e              |
| RIFFELHORN | RFH_0100_04 08 May 19 19:18 | RFH_0100_04 08 May 19 19:18 |
| CODECHIP  | 2019-09-10T17:00:08+0700 | 2019-09-10T17:00:08+0700 |
+-----+-----+-----+
```

Managing software license keys

This chapter provides the following procedures:

- [“Installing a license key” on page 5-2](#)
- [“Installing a license key using a license file” on page 5-4](#)
- [“Installing a license key file with the command file” on page 5-7](#)
- [“Uninstalling a license key” on page 5-8](#)

Procedure 5-1

Installing a license key

You can install a premium feature license key directly by identifying the license key and module number. When the module number is left unspecified, the value defaults to 1.

Step	Action
------	--------

1	Install a premium feature license key: <pre>software license install [file <String>] [server <IP address or host name>][license-key <String[14]>] [module <NUMBER: 1..3>] {default-server default-ftp-server default-tftpserver default-sftp-server {tftp-server <ip-host-str> [server-port <INTEGER: 1...65535>}} {ftp-server <ip-host-str> [login-id <username> [<password-attr> <echolesspassword-attr>][server-port <INTEGER: 1...65535>}} {sftp-server <ip-host-str> login-id <username> {<password-attr> <echolesspassword-attr>}[server-port <INTEGER: 1...65535>}}}</pre> where <table> <tbody> <tr> <td>file <String></td> <td>is the license filename and path.</td> </tr> <tr> <td>server <IP address or host name></td> <td>is the TFTP server.</td> </tr> <tr> <td>license-key <String[14]></td> <td>is the license key string.</td> </tr> <tr> <td>module <NUMBER: 1..3></td> <td>is the module number.</td> </tr> <tr> <td>default-server</td> <td>uses the default xFTP server.</td> </tr> <tr> <td>default-ftp-server</td> <td>uses the default FTP server.</td> </tr> <tr> <td>default-tftp- server</td> <td>uses the default TFTP server.</td> </tr> <tr> <td>default sftp- server</td> <td>uses the default SFTP server.</td> </tr> <tr> <td>tftp-server <ip- host-str></td> <td>is the tftp-server.</td> </tr> </tbody> </table>	file <String>	is the license filename and path.	server <IP address or host name>	is the TFTP server.	license-key <String[14]>	is the license key string.	module <NUMBER: 1..3>	is the module number.	default-server	uses the default xFTP server.	default-ftp-server	uses the default FTP server.	default-tftp- server	uses the default TFTP server.	default sftp- server	uses the default SFTP server.	tftp-server <ip- host-str>	is the tftp-server.
file <String>	is the license filename and path.																		
server <IP address or host name>	is the TFTP server.																		
license-key <String[14]>	is the license key string.																		
module <NUMBER: 1..3>	is the module number.																		
default-server	uses the default xFTP server.																		
default-ftp-server	uses the default FTP server.																		
default-tftp- server	uses the default TFTP server.																		
default sftp- server	uses the default SFTP server.																		
tftp-server <ip- host-str>	is the tftp-server.																		

where

server-port <INTEGER: 1..65535>	is the server-port number.
ftp-server <IP- host-str>	is the ftp-server-name.
login-id <username>	is the FTP/SFP user name.
password-attr	enters the password in clear text.
echoless- password attr	engages an echoless password collector.
sftp-server <IP- host-str>	is the sftp-server name.

—end—

Example

The following example installs a license key with implied module 1:

```
software license install license-key W123XYZ123XYZY
```

The following example installs a license key with module 2:

```
software license install license-key W123XYZ123XYZY module 2
```

Procedure 5-2

Installing a license key using a license file

You can install a license key by specifying a license file, which identifies

- license key
- module

The license key is installed by specifying the license file and the server that the license file is to be downloaded from.

One or more license keys can be stored in a single license file: there is no restriction on the number of license keys stored in a license file.

The format of a license file consists of each new line containing:

```
install <KeyString> <ModuleNumber>
uninstall <FeatureName> <ModuleNumber>
```

The following example shows lines in a license file:

```
install W123XYZ123XYZY    ! module 1 is implied
install W123XYZ123XYZA 2 ! module 2
uninstall MPLS            ! all keys for feature name removed
uninstall MPLS    3      ! only key for feature name
on module 3 removed
```

Any text following an exclamation point (!) is a comment, and spaces are ignored.

Step Action

- 1** Install a license key using a license file:
- ```
software license install file <String> server <IP address
or host name> [license-key <String[14]>] [module <NUMBER:
1-3>]

{default-server|default-ftp-server|default-
tftpserver|default-sftp-server|

{tftp-server <ip-host-str> [server-port <INTEGER:
1...65535>]}|

{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echolesspassword-attr>] [server-port
<INTEGER: 1...65535>]}|

{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echolesspassword-attr>} [server-port
<INTEGER: 1...65535>}]}
```

where

|                                  |                                                                    |
|----------------------------------|--------------------------------------------------------------------|
| file <String>                    | is the license filename and path.                                  |
| server <IP address or host name> | is the TFTP server that the license file is to be downloaded from. |
| license-key <String[14]>         | license key string.                                                |
| module <NUMBER: 1-3>             | module number.                                                     |
| default-server                   | uses the default xFTP server.                                      |
| default-tftp-server              | uses the default TFTP server.                                      |
| default-ftp-server               | uses the default FTP server.                                       |
| default sftp-server              | uses the default SFTP server.                                      |
| tftp-server <IP-host-str>        | is the tftp-server.                                                |
| server-port <INTEGER" 1..65535>  | is the server-port number.                                         |
| ftp-server <<IP-host-str>        | is the ftp-server name.                                            |
| login-id <username>              | is the FTP/SFP username.                                           |

## 5-6 Managing software license keys

---

where  
password-attr      enters the password in clear text.  
echoless-           collects the password interactively.  
password-attr  
sftp-server <IP-      is the sftp-server name.  
host-str>

—end—

### Example

The following example installs a license with a license file:

```
software license install file license.txt server 192.0.2.0
```

System response:

```
WORKING: downloading file remote license.txt local /tmp/temp2
```

---

## Procedure 5-3

### Installing a license key file with the command file

---

The device looks for the license file tag in the XML file and it downloads and processes all licenses specified in the license file. A sample XML file is shown below.

```
<XmlWwpCommandFile>
 <XmlCmdPlatformClass name="CN3942"
 version="saos-<build>"
 operation="upgrade"
 serviceAffecting="yes">
 </XmlCmdPlatformClass>
 <XmlCmdPlatformClass name="caliondo"
 configFilePath="myFolder/my-config-file.txt"
 configFileRule="activate"
 welcomeBanner="myBannerFile.txt"
 licenseFile="myLicenseFile.txt"
 version="saos-<build>"
 packagePath="folder1/folder2/folder3"
 operation="install"
 serviceAffecting="no"
 ftpConfigFile="ciena/defaultFtpConfig">
 <SshKeyFile name="user1.pk2"></SshKeyFile>
 <SshKeyFile name="user2.pk2"></SshKeyFile>
 <SshKeyFile name="user3.pk2"></SshKeyFile>
 </XmlCmdPlatformClass>
</XmlWwpCommandFile>
```

## Procedure 5-4

### Uninstalling a license key

---

Uninstall a license key when the license key is no longer required.

Step	Action
1	Uninstall a license key:  <pre>software license uninstall feature-name &lt;String[32]&gt; module &lt;NUMBER: 1..3&gt;</pre>  where   feature-name      is the premium feature name. &lt;String[32]&gt;   module            is the module number. &lt;NUMBER: 1..3&gt;
2	To display the status of licenses, enter the following command:  <pre>software license show</pre>  —end—

### Example

The following example uninstalls a license key on the entire chassis:

```
software license uninstall feature-name MPLS
```

The following example uninstalls a license key for a specific option module:

```
software license uninstall feature-name MPLS module 3
```

---

## Live patching

---

Live patching delivers corrective content to a switch while the switch is in-service. Corrective content is applied with no impact or minimal impact to the capability of the switch to provide services.

Patch content differs from corrective content load as a corrective content load has multiple software fixes while a patch is an independent fix. Ciena Support will deliver a live patch unit file which is a software file used to apply a software fix to a switch.

All patch applications and patch removals are logged. All patch applications are reported in a state dump.

## Deployment

When a live patch unit file is created, it is deployed to a switch as described in [Table 6-1](#).

**Table 6-1**  
**Deployment steps**

Task	Description
Transfer live patch unit file	Transfers the live patch unit file onto the target switch using existing XFTP commands.
Add the live patch unit file to the live patch system	Validates that the live patch unit file is applicable to the hardware and software it is being applied to.  Verifies any cryptographic signature information included in the live patch unit file.  When completed successfully, the live patch unit file is in the inactive state. No changes have been made to software functionality.
Activate the live patch unit file	Applies the live patch unit file to the running software only if the live patch unit file is in the inactive state.  When completed successfully, the live patch unit file is in the active state. Software functionality has been modified, but the change does not persist over a system restart.
Commit the live patch unit file	Allows the live patch unit file to persist over a system restart.  When completed successfully, the live patch unit file is in the committed state.

The live patch system stores live patch unit files and their state in the active software image bank. This results in the following behavior:

- Live patch unit files are not propagated by a software upgrade.
- Live patch unit files are copied by a software protect operation.
- Live patch unit files persist in a software bank and will be reapplied if the software bank is reactivated.
- Upgrading a software bank with live patch unit files removes the live patch unit files that were installed in the software bank.

## Live patch unit file deactivation and removal

When an active or committed live patch unit files needs to be deactivated, the state of the live patch unit file is changed to inactive. This reverts the corresponding software back to the state it was prior to when the live patch unit file was applied.

The live patch unit file can be removed, however, if it needs to be reapplied, it must be transferred onto the system again.

## Live patch unit queries

The live patch system can query the state and other information associated with a live patch unit file. Each live patch unit file contains information to identify the issue being addressed and a text description that gives more details on the issue and its fix.

## Limitations

The live patch unit file remove commands will fail if the live patch unit file is in use by a running binary. The live patch unit file is considered to be in use by a binary image if the target binary is running while the live patch unit file is in the active or committed state. For live patch unit files which are applied at the SAOS binary, the SAOS server and all CLI instances must be restarted before a live patch unit file can be removed. This requires a reboot.

Live patch functionality is not supported in enhanced security mode.

## Procedure 6-1

### Adding a live patch unit file to the patch database

---

Add a live patch unit file to the patch database.

---

Step	Action
------	--------

---

- |   |                                                   |
|---|---------------------------------------------------|
| 1 | Add a live patch unit file to the patch database: |
|---|---------------------------------------------------|

```
patch add filename <filename>
```

where

filename            is the absolute pathname of the live patch unit file.  
<filename>

—end—

---

## Procedure 6-2

### Removing a patch

---

A live patch unit file must be in the inactive state and not in use before it can be removed from the system. For a live patch unit file to be not in use, all binaries that were affected by the live patch unit file must exit. In most cases, this will require a reboot after the live patch unit file is in the inactive state.

Step	Action
1	Remove a patch: <pre>patch remove patch &lt;patch&gt;</pre> where  patch &lt;patch&gt; is the name of the name of the live path unit file.  —end—

## Procedure 6-3

### Modifying the state of the patch

---

Modify the state of the specified patch.

Step	Action
1	Modify the state of the specified patch:  <pre>patch set &lt;patch&gt; {state &lt;active  inactive committed&gt;}</pre>  where   patch is the name of the name of the live path unit file.   state &lt;activeinactivecommitted&gt; is the state the patch is being set to: active, inactive or committed.   —end—

## Procedure 6-4

### Displaying patches

Use this procedure to troubleshoot any problems.

You can

- display summary information for all patches
- display detailed information for all patches
- display detailed information for a single patch

---

Step	Action
------	--------

---

#### *Display summary information for all patches*

- 1 Display summary information for all patches:

```
patch show
```

#### *Display detailed information for all patches*

- 2 Display detailed information for all patches:

```
patch show all
```

#### *Display detailed information for a single patch*

- 3 Display detailed information for a single patch:

```
patch show <patch-object>
```

where

patch-object is the name of the single live patch unit file.

—end—

### Example

This example shows output from the patch show command:

```
> patch show
```

```
+-----+-----+ PATCH SUMMARY +-----+-----+
| Patch | | | | State | | |
+-----+-----+-----+-----+
| patch1 | | | | committed | | |
| patch2 | | | | active | | |
| patch3 | | | | inactive | | |
+-----+-----+-----+-----+
```

This example shows output from the patch show all command:

## 6-8 Live patching

---

```
> patch show all
```

Patch	patch1
State	committed
Reason	CSR-111111
Binary	leos
Function	n/a
Comment	This is a no-op patch for testing the patch infrastructure.
Patch	patch2
State	active
Reason	CSR-222222
Binary	leos
Function	n/a
Comment	This is a no-op patch for testing the patch infrastructure.
Patch	patch3
State	inactive
Reason	CSR-333333
Binary	leos
Function	n/a
Comment	This is a no-op patch for testing the patch infrastructure.

This example shows output from the patch show command for patch 1:

```
> patch show patch patch1
```

Patch	patch1
State	committed
Reason	CSR-111111
Binary	leos
Function	n/a
Comment	This is a no-op patch for testing the patch infrastructure.





# 39XX/51XX Switches and Platforms

## Software Management and Licensing

Copyright© 2022 Ciena® Corporation. All rights reserved.

SAOS 6.21.2

Publication: 009-3458-018

Document status: Standard

Revision A

Document release date: March 2022

### **CONTACT CIENA**

For additional information, office locations, and phone numbers, please visit the Ciena web site at **[www.ciena.com](http://www.ciena.com)**