39XX/51XX Service Delivery and Aggregation Switches

Software Management and Licensing

SAOS 6.12

What's inside...

New in this release
Software management fundamentals
Managing system software
Software license fundamentals
Managing software license keys

009-3240-018 - Standard Revision A
April 2014

LEGAL NOTICES

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		
In North America	1-800-CIENA24 (243-6224) 410-865-4961	
In Europe, Middle East, and Africa	800-CIENA-24-7 (800-2436-2247) +44-207-012-5508	
In Asia-Pacific	800-CIENA-24-7 (800-2436-2247) +81-3-6367-3989 +91-124-4340-600	
In Caribbean and Latin America	800-CIENA-24-7 (800-2436-2247) 410-865-4944 (USA)	
Sales and General Information	410-694-5700	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	+91-124-434-0500	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training	877-CIENA-TD (243-6283) or 410-865-8996	E-mail: techtng@ciena.com

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

IMPORTANT: PLEASE READ THIS LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE INSTALLING OR USING CIENA CORPORATION (“Ciena”) SOFTWARE, HARDWARE OR DOCUMENTATION (COLLECTIVELY, THE “EQUIPMENT”).

BY INSTALLING OR USING THE EQUIPMENT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Right to Use License; Restrictions. Subject to these terms, and the payment of all applicable license fees, Ciena grants to you, as end user, a non-exclusive license to use the Ciena software (the “Software”) in object code form solely in connection with, and as embedded within, the Equipment,. You shall have the right to use the Software solely for your own internal use and benefit. You may make one copy of the Software and documentation solely for backup and archival purpose, however you must reproduce and affix all copyright and other proprietary rights notices that appear in or on the original. You may not, without Ciena's prior written consent, (i) sublicense, assign, sell, rent, lend, lease, transfer or otherwise distribute the Software; (ii) grant any rights in the Software or documentation not expressly authorized herein; (iii) modify the Software nor provide any third person the means to do the same; (iv) create derivative works, translate, disassemble, recompile, reverse engineer or attempt to obtain the source code of the Software in any way; or (v) alter, destroy, or otherwise remove any proprietary notices or labels on or embedded within the Software or documentation. You acknowledge that this license is subject to Section 365 of the U.S. Bankruptcy Code and requires Ciena's consent to any assignment related to a bankruptcy proceeding. Sole title to the Software and documentation, to any derivative works, and to any associated patents and copyrights, remains with Ciena or its licensors. Ciena reserves to itself and its licensors all rights in the Software and documentation not expressly granted to you. You shall preserve intact any notice of copyright, trademark, logo, legend or other notice of ownership from any original or copies of the Software or documentation.

2. Audit: Upon Ciena's reasonable request, but not more frequently than annually without reasonable cause, you shall permit Ciena to audit the use of the Software at such times as may be mutually agreed upon to ensure compliance with this Agreement.

3. Confidentiality. You agree that you will receive confidential or proprietary information (“Confidential Information”) in connection with the purchase, deployment and use of the Equipment. You will not disclose Confidential Information to any third party without prior written consent of Ciena, will use it only for purposes for which it was disclosed, use your best efforts to prevent and protect the contents of the Software from unauthorized disclosure or use, and must treat it with the same degree of care as you do your own similar information, but with no less than reasonable care. You acknowledge that the design and structure of the Software constitute trade secrets and/or copyrighted materials of Ciena and agree that the Equipment is Confidential Information for purposes of this Agreement.

4. 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 Equipment and any accompanying technical data (collectively “Materials”) are commercial within the meaning of applicable Federal acquisition regulations. These Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this Agreement, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, software delivered to you is commercial computer software and the use of that software is further restricted by this Agreement.

5. Term of License. This license is effective until terminated. Customer may terminate this license at any time by giving written notice to Ciena [or] and destroying or erasing all copies of Software including any documentation. Ciena may terminate this Agreement and your license to the Software immediately by giving you written notice of termination in the event that either (i) you breach any term or condition of this Agreement or (ii) you are wound up other than voluntarily for the purposes of amalgamation or reorganization, have a receiver appointed or enter into liquidation or bankruptcy or analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. In the event of any termination you will have no right to keep or use the Software or any copy of the Software for any purpose and you shall destroy and erase all copies of such Software in its possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased.

6. Compliance with laws. You agree to comply with all applicable laws, including all import regulations, and to obtain all required licenses and permits related to installation and use of Equipment. Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

7. Limitation of Liability. ANY LIABILITY OF Ciena SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU 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 THIRD-PARTY SUPPLIER OF Ciena. NEITHER Ciena NOR ANY OF ITS THIRD-PARTY SUPPLIERS 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

8. General. Ciena may assign this Agreement to any Ciena affiliate or to a purchaser of the intellectual property rights in the Software, but otherwise neither this Agreement nor any rights hereunder may be assigned nor duties delegated by either party, and any attempt to do so will be void. This Agreement shall be governed by the laws of the State of Maryland (without regard to the conflict of laws provisions) and shall be enforceable in the courts of Maryland. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This Agreement constitutes the complete and exclusive statement of 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.

Contents

New in this release 2-1

Software management fundamentals 3-1

Overview 3-1
Network connectivity and xFTP server settings 3-1
System software package 3-1
File naming conventions 3-2
Release compatibility 3-3
xFTP package directory 3-3
Command files 3-5
  Command file types 3-5

Managing system software 4-1

List of procedures

3-1 Specifying xFTP server settings 4-3
3-2 Transferring files 4-6
3-3 Upgrading using the CLI and a command file 4-9
3-4 Upgrading using the CLI without a command file 4-13
3-5 Upgrading using a DHCP server 4-17
3-6 Upgrading using the software install command 4-19
3-7 Backing up software images 4-23

Software license fundamentals 5-1

Managing software license keys 6-1

List of procedures

5-1 Installing a license key 6-2
5-2 Installing a license key using a license file 6-4
5-3 Installing a license key file with the command file 6-6
5-4 Uninstalling a license key 6-7

Publication history

April 2014

Revision A Standard

First Standard release of this document for SAOS 6.12

About this document

This manual describes software management and licensing on 39XX/51XX Service Delivery and Aggregation Switches. 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 platforms.

This manual provides information and examples for use in configuring system software on any platform 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 Service Delivery and Aggregation Switches documentation suite, see *39XX/51XX Service Delivery and Aggregation Switches Product Fundamentals* (009-3240-006).

New in this release

The following sections summarize documentation changes in *Software Management and Licensing* (009-3240-018) for software features introduced with SAOS 6.12.

Advanced Synchronization License support (5150)

- “Software License Keys and Features” on page 4-2

RADIUS Accounting

- “Software License Keys and Features” on page 4-2

Software management fundamentals

This chapter describes software management for upgrading and downgrading 39XX/51XX Service Delivery and Aggregation Switches.

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 to 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 will be 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.

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>-3916_3930_3931_5142.tar.gz	Backwards-compatible image files for 3916, 3930, 3931, and 5142
le-<Image ID>-3916_3930_3931_5142.tar.xz	Complete set of image files for 3916, 3930, 3931, and 5142
le-<Image ID>-3932.tar.xz	Complete set of image files for 3932
le-<Image ID>-3940_3960_5140.tar.gz	Backwards-compatible image files for 3940, 5140, 3960
le-<Image ID>-3940_3960_5140.tar.xz	Complete set of image files for 3940, 5140, 3960
le-<Image ID>-5150.tar.gz	Backwards-compatible image files for 5150
le-<Image ID>-5150.tar.xz	Complete set of image files for 5150
le-<Image ID>-5160.tar.gz	Backwards-compatible image files for 5160
le-<Image ID>-cavium.ins	Upgrade install script for 3916, 3930, 3931, 3932, 5142, 5150 and 5160 platforms
le-<Image ID>.chk	Upgrade check script
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

Release compatibility

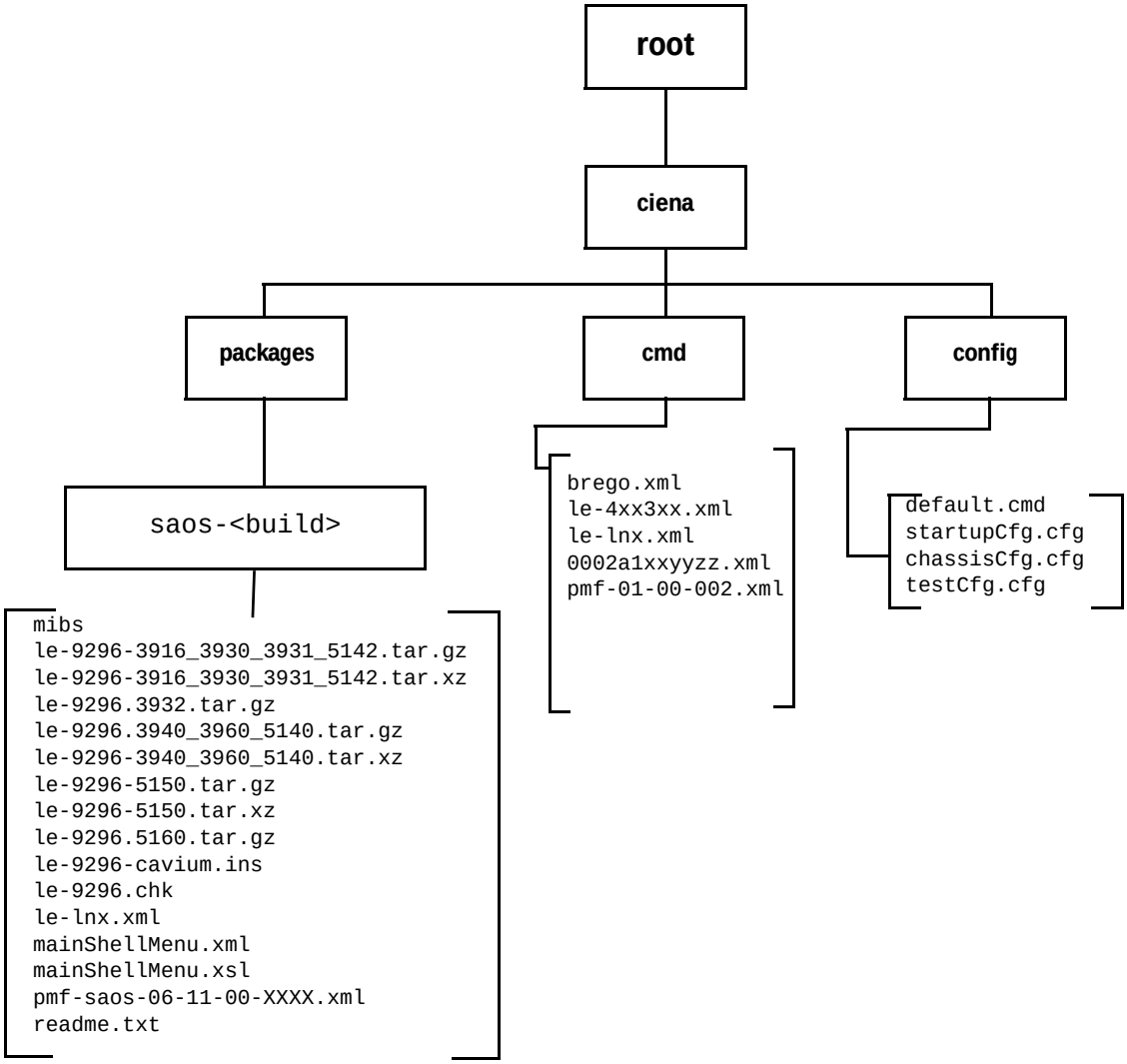
The following rules apply to software upgrade:

- Upgrade and downgrade between 6.12x, 6.11.x, and 6.10x is fully supported and tested on the 3916, 3930, 3931, 3940, 3960, 5140, and 5150 switches.
- Upgrade and downgrade between releases 6.12.x and 6.11.x is fully supported and tested on the 3932, 5142 and 5160 switches.
- Upgrade and downgrade between releases 6.11.x, 6.10.x, and 6.9.x is fully supported and tested on the 3916, 3930, 3931, 3940, 3960, 5140, and 5150 switches.
- Upgrade and downgrade between releases 6.10.x, 6.9.x, and 6.8.x releases 6.8.0.264 or later is fully supported on the 3916, 3930, 3931, 3940, 3960, 5140, and 5150 switches. The 3932, 5142, and 5160 platforms cannot be downgraded to any release prior to 6.11.0.
- Upgrade and downgrade between releases 6.8.x, 6.7.x, and 6.6.x is fully supported and tested on the 3940, 3960, and 5140 platforms.
- Upgrade and downgrade between releases 6.8.x and 6.7.x is fully supported and tested on the 5150 platform.
- The 3916, 3930, and 3931 platforms cannot be downgraded to any release prior to 6.8.0.
- Switches will not install unsupported software.
- Attempting to install unsupported software causes an error message.

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-06-12-00-XXXX). The recommended file structure for the xFTP package directory is <xftproot>/ciena/packages/ (where <xftproof> is a sub-directoroy 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 platform 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 platform 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 platform class command file named le-lnx.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 platform classes. Device specific command files are named with the device MAC address, such as:

- 0002a1010203.xml

Platform class command files are named as follows:

- brego.xml - for 3940, 3960, and 5140 platforms
- caliondo.xml - for 3916, 3930, 3931, 3932, 5142, 5150, and 5160 platforms

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 platform-class.  You may define as many platform classes as you like
in a single command file.

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

<XmlWwpCommandFile>
    <XmlCmdPlatformClass name="CN3916"
        version="saos-<build>"
        operation="upgrade"
        serviceAffecting="yes">
    </XmlCmdPlatformClass>
    <XmlCmdPlatformClass name="brego"
        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 attributes are MANDATORY:
    platformClass
   in order of preference, the most specific match (eg, CN3916), then the class
   match (eg, brego for CN3940 CN5140, and CN3960, caliondo for CN5150, 3916,
        3930, 3931, 3932, 5142, and 5160)

Possible values for platformClass:
  CN3940, CN5140, CN3960, CN5150, 3916, 3930, 3931, 3932, 5142, 5160, brego, caliondo.

The following attributes are OPTIONAL:
    configFilePath          (path and filename, path is relative to tftproot)
    configFileRule          (see note #1 below)
    welcomeBanner           (path and filename, path is relative to tftproot)
    licenseFile             (path and filename, path is relative to tftproot)
    SshKeyFile              (path and filename, path is relative to tftproot)
    version                 (leos-xx-yy-zz-abcd)
    packagePath             (complete path to the package directory relative to the
tftp-root directory)
    operation               (upgrade or xgradei or install)
    serviceAffecting        (yes or no)
   ftpConfigFile          (path and filename, path is relatve to ftp/sftp/tftp root,
see note #3 below)

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
    upgrade
        - Download & 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 & install image files if necessary
        - Do not activate the new image files
        - This option is not available for CN3911, CN3920, and 3902
    x-grade
        - Exact same behavior as 'upgrade'
        - It is supported for backwards compatibility with previous release.
    download
```

```
        - Download image files if necessary
        - Do not install the new image files
         - Image files will be installed after next reboot command.
        - This option is only available for CN3911, CN3920, and 3902
    delete
        - Delete all files that were downloaded for a 2 stage upgrade
        - Cancel 2 stage upgrade and restore device to the default state
        - This option is only avaiable for the CN 3911, CN 3920, and 3902


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 only run the command file 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 commment
    !
    ! 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:10.1.28.62
    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 and install image files if necessary.
  - Activate the new image files.
  - This operation may require a reboot.
  - Reboot does not occur unless serviceAffecting=“yes”.
- install
  - Download and install image files if necessary.
  - Do not activate the new image files.
- x-grade
  - Same behavior as upgrade.

– It is supported for backwards compatibility with previous releases.

Note: If you intend to upgrade software AND system configuration with the same command file, do NOT use 'activate' for the configFileRule.

Instead of using activate for the configFileRule when upgrading software AND system configuration with the same command file, use one of the following combinations:

- 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.

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"
```

Managing system software

The in-service-software upgrade keeps the data plane up and running while a system is performing a software upgrade. Layer 2 traffic continues to flow while the system upgrades its software and reboots. A management plane outage still occurs.

The in-service software upgrade is supported on the 3916, 3930-910, 3930-930, 3931, 3932, 3960, 5142, 5150 and 5160.

There are two types of resets: fast-start (default) and cold-start. A fast-start reset is a control plane reset of the CPU, RAM, NOR flash and NAND flash. This also entails skipping POST. 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 it is specified during a software upgrade or reboot.

In-service-software upgrade is a phased-in implementation. The 6.12 release measures and reduces the outage. Layer 2 forwarding outage times are reduced by deferring the reset of the switch and data plane FPGAs as much as possible.

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.

This chapter provides the following procedures:

- “Specifying xFTP server settings” on page 3-3
- “Transferring files” on page 3-6
- “Upgrading using the CLI and a command file” on page 3-9
- “Upgrading using the CLI without a command file” on page 3-13
- “Upgrading using a DHCP server” on page 3-17
- “Upgrading using the software install command” on page 3-19

- “Backing up software images” on page 3-23

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 <xftproot>/ciena/packages/saos-<build> directory on the xFTP server or the upgrade will fail.

Procedure 3-1
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 3-1 lists the attributes for specifying the xFTP server.

Table 3-1
xFTP Server Settings

Designated xFTP server attribute(s)	Description
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.
sftp-server <IpHost>	SFTP server specified by IP address or host name (if DNS is configured).
tftp-server <IpHost>	TFTP server specified by IP address or host name (if DNS is configured).
ftp-server <IpHost>	FTP server specified by IP address or host name (if DNS is configured).
connection-timeout <NUMBER: 1-100>	Time to wait (in seconds) before the retry times out. Default is 5 seconds.
login-id <String[32]>	User name for the xFTP server. Valid for use with SFTP or FTP server. Default user name is “anonymous”. Same as the user attribute.
password <Password String[128]>	Plain text password string for the xFTP server. Valid for use with SFTP or FTP server. Default password is blank.
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.
secret <String[256]>	Encrypted form of the password string for the xFTP server. Valid for use with SFTP or FTP server.

Software management commands that transfer files (such as, upgrade, install, and run), provide attributes to override the configured xFTP server IP host, login-id, password, and secret settings listed in Table 3-1. 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 3-2.

Table 3-2
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 xftp set tftp-server <IpHost>
```

```
system xftp set ftp-server <IpHost> login-id <String>
[password <String[128]>] [secret <String[256]>]
```

```
system xftp set sftp-server <IpHost> login-id <String>
[password <String[128]>] [secret <String[256]>]
```

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
password MyPassword
system xftp set sftp-server 198.51.100.0 login-id
mySFTPuser password MyPassword
system xftp set tftp-server 203.0.113.0
system xftp set mode tftp
system xftp show
```

```
+-------------------------------- XFTP SETTINGS ---------------------------------+
| Default Mode       : tftp                                                      |
| Tftp Host (User)   : 203.0.113.0                                               |
| Tftp Host (DHCP)   :                                                           |
| Tftp Host (Oper)   : 203.0.113.0                                               |
| Ftp Host Name      : 192.0.2.0                                                 |
| Ftp Login ID       : myFTPuser                                                 |
| Sftp Host Name     : 198.51.100.0                                              |
| Sftp Login ID      : mySFTPuser                                                |
| Connection Timeout : 5                                                         |
| Retry Interval     : 15                                                        |
| Retries            : 2                                                         |
+--------------------------------------------------------------------------------+
```

Procedure 3-2
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

1 Transfer files to an xFTP server:

```
system xftp putfile {local-filename <String[63]>}
{remote-filename <String[63]>} default-tftp-server
default-ftp-server default-server default-sftp-server
[sftp-server <IP address or host name>] [tftp-server <IP
address or host name>] [ftp-server <IP address or host
name>] [login-id <String[32]>] [password <Password
String>] [secret <String[256]>]
```

where

local-filename <String[63]>	is the local filename.
remote-filename <String[63]>	is the remote filename.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-server	uses the default xFTP server.
default-sftp-server	uses the default SFTP server.
sftp-server <IP address or host name>	is the SFTP server.
tftp-server <IP address or host name>	is the TFTP server.
ftp-server <IP address or host name>	is the FTP server.

where

login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted string.

To receive files from an xFTP server

2 Receive files from an xFTP server:

```
system xftp getfile {remote-filename <String[63]>}
{local-filename <String[63]>} default-tftp-server
default-ftp-server default-server default-sftp-server
[sftp-server <IP address or host name>] [tftp-server <IP
address or host name>] [ftp-server <IP address or host
name>] [login-id <String[32]> [password <Password
String>] [secret <String[256]>]
```

where

remote-filename <String[63]>	is the remote filename.
local-filename <String[63]>	is the local filename.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-server	uses the default xFTP server.
default-sftp-server	uses the default SFTP server.
sftp-server <IP address or host name>	is the SFTP server.
tftp-server <IP address or host name>	is the TFTP server.
ftp-server <IP address or host name>	is the FTP server.

where

login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted 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 3-3
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.

```
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 Run the command file, specifying the desired directory, command file, and xFTP server attribute(s).

```
software run {command-file <String>} [server <IP address
or host name>] default-tftp-server default-ftp-server
default-server default-sftp-server [sftp-server <IP
address or host name>] [tftp-server <IP address or host
name>] [ftp-server <IP address or host name>] [login-id
<String[32]>] [password <Password String>] [secret
<String[256]>]
```

where

command-file <String>	is the filename of the command file including path.
server <IP address or host name>	is the TFTP server.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-server	uses the default xFTP server.
default-sftp-server	uses the default SFTP server.
sftp-server <IP address or host name>	is the SFTP server.

where

tftp-server <IP address or host name>	is the TFTP server.
ftp-server <IP address or host name>	is the FTP server.
login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted 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. Platform class file for its platform, artimir.xml or brego.xml

c. Generic platform 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 platform 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 a 3960 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
> software run command-file /ciena/packages/saos-<build>/le-lnx.xml default-server
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-<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-
3940_3960_5140.tar.xz local /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: file check ok
WORKING: Installing Image le-8506-3940_3960_5140.tar.xz


Connection to host lost.
CN 3960> soft 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 3-4
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>] [user <String>] [retries <String>] [retry-
interval <String>] [connection-timeout <NUMBER: 1-100>]
[service-disruption <allow|deny>] default-tftp-server
default-ftp-server default-server default-sftp-server
[sftp-server <IP address or host name>] [tftp-server <IP
address or host name>] [ftp-server <IIP address or host
name>] [login-id <String[32]>] [password <Password
String>] [secret <String[256]>] [cold-restart]
```

where

package <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.

where	
user <String>	is the FTP user name.
retries <String>	is the number of retries. Valid values are numbers from 1 to 10.
retry-interval <String>	is the retry interval. Valid values are numbers from 1 to 300.
connection-timeout <String>	is the connection-timeout. Valid values are numbers from 1-100.
service-disruption <allow|deny>	is the service disruption permission.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-server	uses the default xFTP server.
default-sftp-server	uses the default SFTP server.
sftp-server <IP address or host name>	is the SFTP server.
tftp-server <IP address or host name>	is the TFTP server.
ftp-server <IP address or host name>	is the FTP server.
login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted string.
[cold-restart]	optional command that performs a cold-start reset of the control and data plane. The default lis fast-start reset.

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

—end—

Example

The following example upgrades without a command file for a 3960 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-
restart
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-
3940_3960_5140.tar.xz local /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: file check ok
WORKING: Installing Image le-8506-3940_3960_5140.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 3-5
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. Some examples:

- bootfile = “ciena/packages/saos-06-09-00-0126/”
- bootfile = “ciena/packages/saos-06-09-00-0126/command-saos-06-09-00-0126.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 as follows:

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.

```
dhcp client enable
```

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 3-6
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:

```
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 Install the new software package into flash:

```
software install {package <String>} [package-path
<String>] [server <IP address or host name> default-tftp-
server default-ftp-server default-server default-sftp-
server [sftp-server <IP address or host name>] [tftp-
server <IP address or host name>] [ftp-server <IP address
or host name>] [login-id <String32>] [password <Password
String>] [secret <String[256]>]
```

where

package <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 TFTP server.
default-tftp-server	uses the default TFTP server.
default-ftp-server	uses the default FTP server.
default-server	uses the default xFTP server.
default-sftp-server	uses the default SFTP server.

where

sftp-server <IP address or host name>	is the SFTP server.
tftp-server <IP address or host name>	is the TFTP server.
ftp-server <IP address or host name>	is the FTP server.
login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted string.

4 Validate the software:

```
software validate
```

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

```
chassis reboot now [cold-restart]
```

Note: Adding the optional cold-restart 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 fast-start.

6 Confirm the Installed Package and Running Package:

```
software show
```

—end—

Example

This example installs software for a 3960 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
> 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-
3940_3960_5140.tar.xz local /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: tftp file download in progress
WORKING: running check script le-8506.chk on file /tmp/xgrade/images/le-8506-
3940_3960_5140.tar.xz
WORKING: file check ok
WORKING: Installing Image le-8506-3940_3960_5140.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 3-7
Backing up software images

The 3916, 3930, 3931, 3940, 3960, 5140, and 5150 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: `software protect`
2	Confirm information for both flash image banks: `software show`

—end—

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 may consist of a portion of an existing feature, or it may consist of 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.
- The 5150 chassis contains option modules. You can choose to license features for the chassis or for selected option modules.

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 following statuses:

- Not Installed. Also referred to as an invalid license. This means that none of the operationally enabled modules has a key installed for this license.
- Installed. Also referred to as a valid license. This means that all of the operationally enabled modules have a key installed for this license and all conditional requirements (described in separate requirements) for the license installation have been satisfied.
- Partial License. This means that 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 will be generated every 60 minutes until the licenses are installed on all modules.

The following software license keys are available:

- Base Features
- Advanced-Ethernet (AE)
- MPLS
- Advanced-OAM (AOAM)
- Advanced-Security
- PBB-TE
- Advanced-10G (available for 3930, 3931, 3932, and 5142)
- Advanced-Sync (available for 3930, 3930 Sync, 3931, 3932, 5142, 5150, and 5160)

A detailed list of the software license keys and associated features is shown in **Table 4-1**.

Table 4-1
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 3930, 3931, 3932, and 5142 only.) If an NNI port speed is set to 10Gig 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	802.1x Link Aggregation Control Protocol (LACP) as defined in IEEE 802.3ad 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.
Advanced-Ethernet	Broadcast Containment prevents services from being disrupted by broadcast storms on specified ports
Advanced-Ethernet	Configurable L2 Frame Bandwidth Calculation
Advanced-Ethernet	Configurable Metering Burst Size
Advanced-Ethernet	Configurable per-port RED Egress Queuing

Table 4-1
Software License Keys and Features (continued)

Software License Requirement	Feature Description
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)
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.

Table 4-1
Software License Keys and Features (continued)

Software License Requirement	Feature Description
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 4-1
Software License Keys and Features (continued)

Software License Requirement	Feature Description
Advanced-Ethernet	Quality of Service (QoS)-mechanisms for managing bandwidth, including: Traffic Profiling-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-determines the order in which the physical queues are processed. • Configurable Egress Shaping-controls bandwidth for taking frames out of queues at egress. • Configurable frame bandwidth calculation-configure 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 4-1
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 simply 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 (VS) 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 4-1
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 4-1
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 3930, 3930 Sync, 3931, 3932, 5142, 5150, and 5160)
Base-Features	Base Network Time Protocol (NTP)

Table 4-1
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
Base-Features	Trivial File Transfer Protocol (TFTP)
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)
PBB-TE	Provider Backbone Bridge Traffic Engineering (PBB-TE) provides features supported by the IEEE 802.1Qay standard. With PBB-TE, providers can create point-to-point, primary and backup Ethernet tunnels and specify the path that traffic will take across their Ethernet metro networks. These paths reserve appropriate bandwidth and support the provisioned QoS metrics.

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 5-6
- “Uninstalling a license key” on page 5-7

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: `software license install [file <String>] [server <IP Address or host name>][license-key <String>] [module <NUMBER: 1-3>] default-tftp-server default-ftp-server default-server default-sftp-server [sftp-server <IP address or host name>] [tftp-server <IP address or host name>] [ftp-server <IP address or host name>] [login-id <String[32]>] [password <Password String>] [secret <String[256]>]` where file <String> — is the license filename and path. server <IP Address or host name> — is the TFTP server. license-key <String> — is the license key string. module <NUMBER: 1-3> — is the module number. default-tftp-server — uses the default TFTP server. default-ftp-server — uses the default FTP server. default-server — uses the default xFTP server. default-sftp-server — uses the default SFTP server. sftp-server <IP address or host name> — is the SFTP server. tftp-server <IP address or host name> — is the TFTP server. ftp-server <IP address or host name> — is the FTP server.

where

login-id <String[32]>	is the FTP/SFTP username.
password <Password String>	enters the password in clear text.
secret <String[256]>	sets the password using a pre-encrypted string.

—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 PBB-TE       ! all keys for feature name removed
uninstall PBB-TE 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>` where file <String> — is the license file name and path. server <IP address or host name> — is the TFTP server that the license file is to be downloaded from.

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="CN3916"
          version="saos-<build>"
          operation="upgrade"
          serviceAffecting="yes">
     </XmlCmdPlatformClass>
     <XmlCmdPlatformClass name="brego"
          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: `software license uninstall feature-name <String[32]> module <NUMBER: 1-3>` where feature-name <String[32]> is the premium feature name. module <NUMBER: 1-3> is the module number.
2	To display the status of licenses, enter the following command: `software license show`

—end—

Example

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

```
software license uninstall feature-name PBB-TE
```

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

```
software license uninstall feature-name PBB-TE module 3
```

39XX/51XX Service Delivery and Aggregation Switches

Software Management and Licensing

SAOS 6.12
Publication: 009-3240-018
Document status: Standard
Revision A
Document release date: April 2014

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