39XX/51XX Switches and Platforms

Administration and Security

SAOS 6.21.2

What's inside...

009-3458-007 - Standard Revision A
March 2022

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.

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

Standard revision A.

First standard release of this document for SAOS 6.21.2.

Contents

List of procedures

List of procedures

List of procedures

List of procedures

List of procedures

List of procedures

List of procedures

About this document

This document explains tasks performed by operations personnel that are related to the administration of the network and security, including the configuration and management of systems data and users. It also explains how to manage and protect resources from unauthorized or detrimental access and use.

Hyperlinks are indicated by blue text in this document.

To configure Advanced Security features, you need to install the Advanced Security license key. License keys can be purchased by contacting Ciena Customer Support.

Command line interface

The SAOS switch is configured by means of a command line interface (CLI). Topics are:

- “User access” on page xv
- “Command schema” on page xvi
- “Command syntax” on page xvii

User access

The CLI hides commands depending on user access level and installed licenses. When entering a command at the prompt, ensure that you have the appropriate access level.

User access levels are:

- super, for managing secure access to the switch through creation, deletion, and modification of user accounts
- admin, for making significant system state changes, modifying the system configuration, and performing execute commands
- limited, for system monitoring and gathering information about the configuration and performance of the system
- diag, for use when instructed by Ciena Customer Support to gather diagnostic information

This table describes the default user names/passwords provided in the CLI.

Group	User name	Password	Access rights
super	su	wwp	Read/Write/Create
admin	admin	wwp	Read/Write
limited	user	<empty>	Read-Only
diag	gss	pureethernet	Diagnostic

Note 1: Although the default limited user account cannot make configuration changes, the network operator must set a password for the account or delete the account.

Note 2: Default users except "su" are not applicable if the security mode is enhanced (“Enhanced security mode” on page 11-7).

Find more information about user groups in *39XX/51XX Administration and Security.*

Command schema

To provide consistency across all the commands, all CLI commands follow a basic underlying schema:

<object> [<subobject>] <action> [instance] [<attributes>]

This table lists the elements of the command schema and provides a description of each element.

Element	Description
<object>	Identifies a feature or a basic object. On the surface, these seem like completely mismatched entities, however, if a device is considered to have an instance of each of these entities, then both features and the basic system objects are considered as objects.
<subobject>	Subdivides a feature.
<action>	Describes the type of action that occurs on the object or instance specified.
<instance>	Defines an recurrence of an object.
<attributes>	Identifies a pairing of a keyword and a value. A command can take multiple attributes and the attributes can be specified in any order relative to one another.

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.

This table lists the symbols of the command syntax and provides a description of each symbol.

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 can 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`

Symbol	Description

[ ]	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`

{ [ ], [ ], [ ] }	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.

For more information about navigating the CLI, refer to *39XX/51XX Command Reference*.

Related documents

This document is part of a documentation suite that fully describes the 39XX/51XX Switches and Platforms. For more information about 39XX/51XX Switches and Platforms documentation, refer to the documentation roadmap in *39XX/51XX Switches and Platforms Product Fundamentals*.

Trademark acknowledgments

Ciena is a trademark of Ciena Corporation.

New in this release

This section provides a summary of the changes made in *39XX/51XX Switches and Platforms Administration and Security* 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 the procedures in this guide, primarily in the following sections:
    - Chapter 3, “System setup”
    - Chapter 4, “System shell operations”
    - Chapter 6, “Data collection configuration and management”
    - Chapter 10, “Secure communications and infrastructure”
    - Chapter 12, “Security log”

Administration fundamentals

This section provides an overview of these SAOS concepts:

- "User groups" on page 2-1
- "Maximum server connections" on page 2-2
- "Default user names and passwords" on page 2-2
- "System customization" on page 2-3

User groups

User groups provide the framework for secure operation and maintenance of the system.

Every user account is assigned membership to one of three predefined user groups according to recurring tasks to be performed using that account. Each user group has access to command sets based on certain defined areas of responsibility. These user groups are

- "super group" on page 2-1
- "admin group" on page 2-2
- "limited group" on page 2-2

> ***Note:*** A fourth user group (diag) is supported for exclusive use of Ciena's Customer Support Department. It is not a user group intended for use by the network operator. An additional set of special hardware diagnostic commands for use during advanced troubleshooting is only available to this user group. These commands are not required in the operation of the system. In some circumstances, you may be instructed by the Ciena Customer Support Department to gather diagnostic information by logging in as a diag user.

super group

Accounts in this group are used to manage secure access to the switch through the creation, deletion and modification of user accounts. Although users in this group can also make significant system state changes, and modify the configuration, the primary purpose of this group is user account maintenance.

This is the only operational group with access to all user administration commands.

admin group

Accounts in this group are for used to make significant system state changes and modify modifying the system configuration.

limited group

Accounts in this group are used primarily in system monitoring and in the gathering of information about the configuration and performance of the system. A restricted command set protects user accounts in this group from changing the state of the system in a significant way or changing the system configuration.

Maximum server connections

The maximum number of users for the users can be set by the network operator. The number of users for each user group is shared among the Telnet and SSH sessions. The maximum number of users for each user group is shown in this table:

Table 2-1
Maximum server connections

User group	Maximum logged-in-users
Maximum limited users	0 to 9
Maximum admin users	0 to 9
Maximum super users	1 to 10

To specify the maximum number of logged-in-users, see "Setting the maximum server connections" on page 8-6.

Default user names and passwords

The CLI privilege levels table lists the CLI privilege levels and provides the default user name and password for each privilege level.

Table 2-2
CLI privilege levels

Privilege level	User name	Password	Access rights
super	su	wwp	read/write
admin	admin	wwp	read/write
limited	user	<empty>	read-only
diag	gss	pureethernet	diagnostic

Although the default limited user account lacks the privileges to make configuration changes, the network operator may find it wise to set a password for the account. To set a password, see "Modifying a user account" on page 8-7.

CAUTION
At least one user with superuser privilege level must be configured on the device. Before deleting the default superuser account, create another user account with superuser access level.

All SAOS systems set passwords by means of the CLI as an echoless password. An echoless password replaces the traditional password entry. The user is prompted to enter a new password and to verify the password. The cleartext password is never visible anywhere at any time, not even on the network when using SSH.

System customization

SAOS allows you to customize aspects of the system shell, for example, system host name and system time and date. Find system customization procedures in "System shell operations" on page 4-1.

System setup

This section describes system configuration and management.

Protocols are

- IPv4 and IPv6
- Telnet client
- Telnet server
- Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6)
- L2 DHCP relay agent
- L3 DHCP relay agent
- Network Time Protocol
- Neighbor Discovery Protocol

IPv4 and IPv6

Devices communicate by means of IPv4 or IPv6.

IPv6 is the successor to IPv4. IPv6 provides a larger address space and greater flexibility when assigning addresses. IPv6 is not a superset of IPv4 but a new suite of protocols.

Telnet client

Devices support a Telnet client for establishing Telnet connections to other Telnet servers specified by a host name or IPv4 or IPv6 address.

Procedures for the Telnet client are:

- “Running the Telnet client” on page 3-30
- “Telneting to another system using Telnet client” on page 3-31

Telnet server

Telnet server enables support for users to connect to the switch using Telnet client protocol.

> ***Note:*** When Telnet/SSH session back-to-back requests occur in a short period of time, the Telnet/SSH server actively refuses connections to prevent Denial of Service (DoS) attacks. You can configure the maximum DoS protection limit for such telnet sessions. Automatic provisioning systems that provision devices with rapid, successive Telnet/SSH session connections can trigger this DoS protection. To avoid session denial, wait 10 seconds between Telnet/SSH provisioning session requests.

The procedure for Telnet server is:

- "Configuring Telnet" on page 3-26

Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6)

SAOS devices support DHCPv4 or DHCPv6.

IETF RFC 2131 Dynamic Host Configuration Protocol (DHCP) client interface is supported for IPv4 address assignment and other IPv4 configurations through DHCP options. By default, DHCP is enabled on the remote management interface.

IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a network protocol that is used for configuring IPv6 hosts with IP addresses and other configuration information required to operate on an IPv6 network. By default, DHCPv6 is enabled on the remote management interface.

> ***Note:*** DHCPv4 and DHCPv6 can each be connected to only one interface at a time, but they can both be connected to the same or different interfaces at the same time.

DHCPv4 interfaces to these protocols and managers:

- Software Management
- NTP
- Interface Config
- Syslog
- DNS
- ARP
- TFTP/SFTP

DHCPv6 interfaces to these protocols and managers:

- Software Management
- NTP
- Interface Config
- DNS

- TFTP

When you enable DHCP on an interface, it creates a query and sends it to the DHCP server to receive IP configuration. The server replies with the IP address and any configured DHCP options.

The DHCP client checks to see if the IP address is already in use by sending a gratuitous Address Resolution Protocol (ARP). If it is in use, it sends a decline and re-starts the discover process. When DHCP is disabled, any configuration set through DHCP options are deleted. The configuration and options applied as a result of DHCP are not saved in the configuration file. A reboot requires a new DHCP transaction with the server.

DHCPv6 servers receive messages from clients using a reserved, link-scoped multicast address. A DHCPv6 client transmits most messages to this reserved multicast address, so that the client need not be configured with the address or addresses of DHCPv6 servers.

DHCPv6 employs a larger option code space and DHCPv6 options are TLV similar to those in DHCPv4. DHCPv6 uses a 16 bit option type code and length with variable length data. Most information is carried in options, instead of fixed header fields.

The DHCP client supports the DHCP options summarized in the Supported DHCP options table. A complete list of DHCP options is defined in RFC 1533.

Table 3-1
Supported DHCP options

Option #	Name	Description
1	subnet	Specifies the subnet mask for the interface. The default value is on.
2	time-offset	Specifies the offset of the client's clock in seconds from Coordinated Universal Time (UTC). The default value is on.
3	router	Specifies a list of IP addresses for routers (gateways) on the client's subnet. Routers should be listed in order of preference. The default value is on.
6	dns	Specifies a list of five Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers should be listed in order of preference. The default value is on.

Table 3-1
Supported DHCP options

Option #	Name	Description
7	log-server	Specifies a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference. Used by Syslog. Note that this DHCP option provides no mechanism to configure the UDP port for a syslog server. Any syslog servers configured by DHCP use the default UDP port for syslog. The default value is on.
12	host-name	Specifies the name of the client. The name may or may not be qualified with the local domain name. The default value is on.
15	domain-name	Specifies the domain name that client can use when resolving host names via the Domain Name System (DNS). The default value is on.
42	ntp	Specifies a list of IP addresses indicating Network Time Protocol (NTP) servers available to the client. Servers should be listed in order of preference. The default value is on.
51	lease-time	Requests the lease time for the IP address. The default requested client lease-time is 1 hour and the default for this option is off.
66	tftp-server	Identifies a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options. The TFTP address is only used to retrieve the command file and then is discarded. The default value is on.
67	bootfile	Identifies a bootfile, that is, the command file. The default value is on.

Procedures for the DHCP client are:

- “Configuring DHCP client” on page 3-32
- “Configuring the DHCPv6 client” on page 3-37
- “Configuring DHCPv6 client options” on page 3-39
- “Enabling DHCPv6 client rapid commit” on page 3-40
- “Displaying DHCPv6 client information” on page 3-41

DHCPv6

DHCPv6 is a network protocol that is used for configuring IPv6 hosts with IP addresses, IP prefixes and/or other configuration required to operate on an IPv6 network. DHCPv6 is not simply an upgrade to DHCPv4, but is a separate and distinct protocol.

IPv6 hosts can acquire IP addresses using stateless address autoconfiguration, or by using DHCPv6. DHCP tends to be preferred at sites where central management of hosts is valued; stateless autoconfiguration does not require any sort of central management, and is therefore preferable in networks where no management is readily available, such as a typical home network.

With DHCPv6, when the interface generates a query, it receives an RA (router advertisement) from the server which tells it how to get an address based on an the M and O bits set in the RA. If the M bit is set, then the client sends out a request to the server, accepts the address, and sends a message confirming the choice. The server then acknowledges that it has recorded the address. If the M bit is not set, the client does not request an address from a DHCPv6 server.

The signals used for DHCPv6 are also different than in DHCPv4 and the protocol adds features not present in DHCPv4. Some features include:

- IPv6 hosts have "linklocal addresses". Every network interface has a unique address that can be used to send and receive on the link only. IPv6 hosts can use this to send requests for "real" addresses.
- All IPv6 systems support multicasting. All DHCPv6 servers register that they want to receive DHCPv6 multicast packets. This means the network knows where to send them. In IPv4, clients broadcast their requests, and networks do not know how far to send them.
- One exchange configures all interfaces. A single DHCPv6 request includes all interfaces on a client. This allows the server to offer addresses to all interfaces in a single exchange. Each interface can also have different options.
- DHCPv6 defines address allocation types. allowing normal address allocation as well as temporary address allocation.

Procedures for DHCPv6 are:

- “Configuring the DHCPv6 client” on page 3-37
- “Configuring DHCPv6 client options” on page 3-39
- “Enabling DHCPv6 client rapid commit” on page 3-40
- “Displaying DHCPv6 client information” on page 3-41

L2 DHCP relay agent

In the residential, metropolitan Ethernet-access environment, DHCP centrally manages the IP address assignment for a large number of subscribers. The DHCP relay agent adds information to the DHCP request that can be used by the DHCP server to assign addresses.

There are two types of DHCP relay agents which can be used independently or together:

- Layer 2 (L2) DHCP relay agent
- Lightweight DHCPv6 relay agent (LDRA)

L2 relays are created on VLANs or virtual switches. This table describes the VLAN/virtual switch support on SAOS devices for L2 DHCP relay agent and LDRA.

Table 3-2
L2 DHCP and LDRA device support

Device	L2 DHCP relay agent	LDRA
3903, 3903x, 3904, 3905, 3906	VLAN/virtual switch ***Note:*** The virtual switch relay for these devices supports Q-in-Q, but not MPLS-VC.	VLAN/virtual switch ***Note:*** The virtual switch relay for these devices supports Q-in-Q, but not MPLS-VC.
3926, 3928, 3942, 5142, 5160	VLAN/virtual switch	VLAN/virtual switch

The maximum number of relay agents is the total of L2 DHCP relay agents and LDRA. This table lists the maximum number of relay agents and ports for each VLAN by platform.

Table 3-3
Maximum number of relay agents and ports for each VLAN by platform

Platform	Maximum number of relay agents	Maximum number of ports for each VLAN
3903, 3903x, 3904, 3905, 3906, 3926, 3928, 3942, 5142, 5160	512	Maximum number of ports plus maximum number of aggregation ports

L2 DHCP relay agent

L2 DHCP relay agent comprises:

- DHCP option 82

- DHCP broadcast containment

DHCP option 82

DHCP option 82 provides a mechanism for generating IP addresses based on the location of the client device in the network. Information about the location of the device is sent with DHCP requests to the server. An option 82-aware DHCP server analyzes the option 82 information and determines the IP address to assign. DHCP option 82, DHCP L2 Relay Agent information field, is described in RFC 3046.

This table lists the supported sub-options of option 82.

Table 3-4
Supported sub-options of option 82

Subfield	Description
Agent Circuit ID/ Interface ID (VLAN and VS relays)	Specifies the circuit ID type for the L2 DHCP relay agent. The value used for Circuit-ID depends on the circuit-id-type set for the relay agent. There are three different types: • slot-port • slot-port-vlan • cid-string, which is a variable length string of up to 64 characters The value in option 82 is a variable length string: for slot-port it is <slot>.<port> for slot-port-vlan the string is <slot>.<port>.<vlan>. If the request arrives on an aggregation, the <slot>.<port> portion is replaced with the name of the aggregation.
Agent Remote ID (VLAN or VS-based relay)	Specifies the remote ID type for the L2 DHCP relay agent. The value used for the Remote-ID depends on the remote-id-type set for the relay agent. There are three different types: • device-mac • device-hostname • rid-string, which is a variable length string of up to 64 characters

DHCP broadcast containment

Subscribers are identified by the switch port that they connect to the network through, rather than by MAC address. When DHCP option-82 is enabled on a VLAN and client ports are in that VLAN, port-to-port DHCP broadcast is isolated.

For client-to-server exchanges, broadcast requests from clients connected to VLAN access ports are intercepted by the relay agent and are not flooded to other clients on the same VLAN. The relay agent forwards the request to the DHCP server.

For server-to-client exchanges, the DHCP server sends a broadcast reply that contains the option-82 field. The relay agent uses this information to identify the port that connects to the requesting client and avoids forwarding the reply to the entire VLAN.

L2 DHCP relay agents can be used to reduce DHCP broadcast traffic and spoofing attacks by using trusted ports and option 82. Port trust is used to determine whether a port or group of ports can be trusted when analyzing client DHCP broadcasts. A list of trusted client ports and a list of trusted server ports can be configured manually.

This table lists L2 DHCP relay agent trust modes.

Table 3-5
L2 DHCP relay agent trust modes

Trust mode	Description
untrusted	DHCP client messages that do not already contain option82 are relayed. DHCP client messages that contain option82 are dropped. Server DHCP messages that include option 82 are also dropped. Server DHCP messages without option 82 are forwarded to the client ports.
client-trusted	Client DHCP messages are relayed. Server DHCP messages with option 82 are dropped. Server DHCP messages without option 82 are forwarded to the client ports. For virtual switch relays, MPLS-VC interfaces cannot be defined as client-trusted.
server-trusted	All client DHCP messages are dropped. All server DHCP messages are forwarded to the client ports.
dualrole-trusted	For client DHCP messages, dualrole-trusted mode functions the same as client-trusted mode. For server DHCP messages, dualrole-trusted mode functions the same as server-trusted mode. For virtual switch relays, MPLS-VC interfaces cannot be defined as client-trusted.

Trusted and untrusted ports in a ring topology

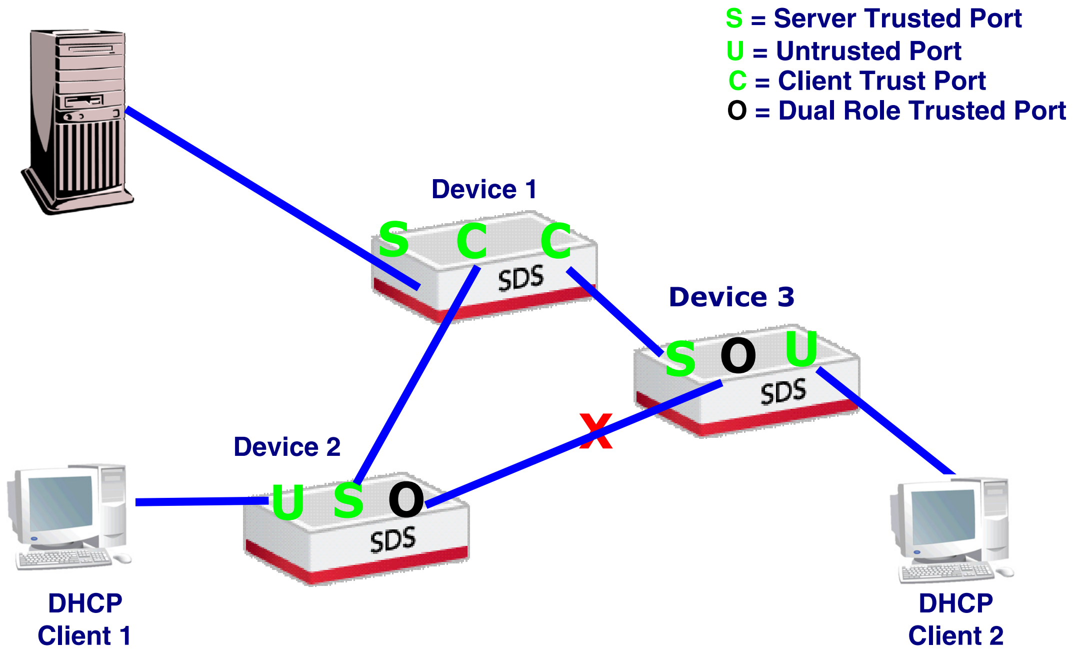
When DHCP clients access the DHCP server by means of a ring topology there is the potential that the client device may become isolated from the server if configured using traditional trusted ports. The dualrole trusted ports feature allows a connecting port to serve as a trusted or untrusted server or a client port as needed.

For example, in the DHCP trusted and untrusted ports in a ring topology figure, assume that the untrusted server port on Device 3 marked with an X is blocked by RSTP and its second port in the ring has been configured as a

DHCP trusted server port. In the event that the link between Device 1 and Device 2 fails, Device 2 needs to receive DHCP server messages from Device 3. The connecting port needs to be configured as a second untrusted server port. In addition, the link partner on Device 3 (the port marked with the letter U) needs to be configured as an untrusted client port.

However, if the link between Device 1 and Device 3 fails, the port on Device 3 (marked with the letter U) needs to become an untrusted server port while its link partner on Device 2 needs to become a client port. They can be configured as one role or the other depending on the scenario.

Figure 3-1
DHCP trusted and untrusted ports in a ring topology



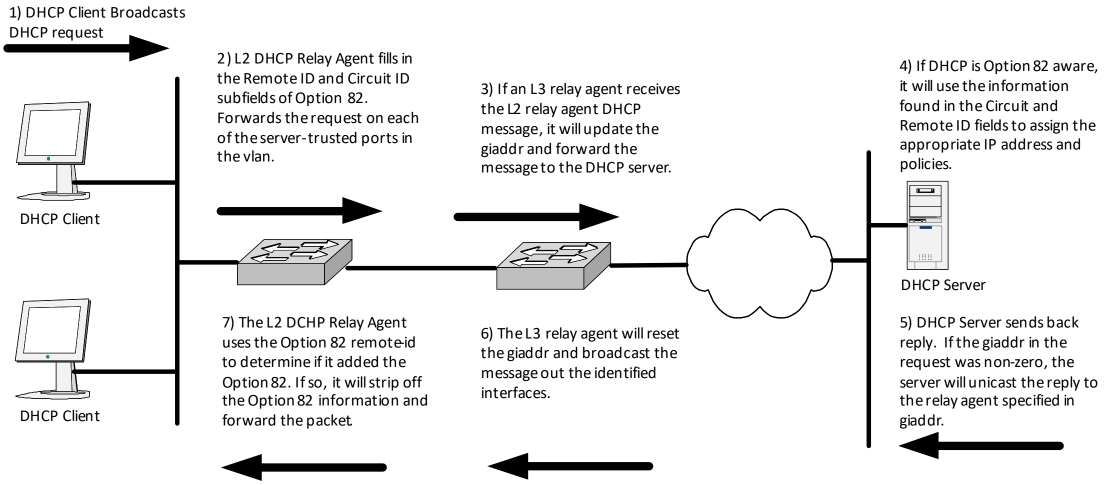
To limit DHCP broadcasts, these rules are enforced when analyzing DHCP broadcasts:

- Intercept DHCP discover messages and forward them only to the trusted server ports in the VLAN.
- Intercept DHCP broadcast requests and forward them only to the trusted server ports in the VLAN.
- Intercept DHCP broadcast replies and forward them only to the trusted client ports in the VLAN. However, if option 82 information referencing an untrusted client port is present in the reply, the reply is forwarded to the untrusted client port.

- Intercept unicast DHCP discover messages. Discard a frame if it is a unicast discover and its IP address is spoofed, that is, non-zero, to look like it came from a relay agent and it arrives on an untrusted server port.

This figure shows L2 relay.

Figure 3-2
Simple network diagram with L2 relay


1) DHCP Client Broadcasts DHCP request
2) L2 DHCP Relay Agent fills in the Remote ID and Circuit ID subfields of Option 82. Forwards the request on each of the server-trusted ports in the vlan.
3) If an L3 relay agent receives the L2 relay agent DHCP message, it will update the giaddr and forward the message to the DHCP server.
4) If DHCP is Option 82 aware, it will use the information found in the Circuit and Remote ID fields to assign the appropriate IP address and policies.
DHCP Client
DHCP Server
DHCP Client
7) The L2 DCHP Relay Agent uses the Option 82 remote-id to determine if it added the Option 82. If so, it will strip off the Option 82 information and forward the packet.
6) The L3 relay agent will reset the giaddr and broadcast the message out the identified interfaces.
5) DHCP Server sends back reply. If the giaddr in the request was non-zero, the server will unicast the reply to the relay agent specified in giaddr.

Procedures for the Layer 2 DHCP relay agent are:

- “Configuring the L2 DHCP relay agent” on page 3-43
- “Creating lists of trusted client ports and server ports” on page 3-48

Lightweight DHCPv6 relay agent

Lightweight DHCPv6 relay agent (LDRA) provides relay agent information from access nodes that are performing bridging, that is, non-routing, operations. LDRAs are created on VLANs or virtual switches as outlined in Table 3-5. Lightweight DHCPv6 relay agents are a mechanism for providing the DHCPv6 server with relay agent information that can be used for client identification. LDRAs are created on VLANs or virtual switches. LDRA does not require IPv6 routing or control functions so it can be implemented on Ethernet switches. Since the LDRA does not route, it must reside on the same link as the client or client-facing DHCPv6 relay agent, and the server or server-facing DHCPv6 relay agent.

Information provided by LDRA can be used by the DHCPv6 server for assigning an IP address based on the location of the client device in the network. LDRA adds the interface-ID option to messages directed toward the DHCPv6 server. The interface-ID option identifies the client-facing interface that the relay received the message on.

This table lists LDRA attributes.

Table 3-6
LDRA attributes

Attribute	Description
interface-id-type	Identifies the interface that the client-originated packet was received on. When the LDRA forwards a client-originated DHCPv6 packet, it encapsulates the received message in a relay-message option, and adds the interface-id option (option 18). The value is a variable length string. Valid values are: • slot-port, formatted as <slot>.<port> • slot-port-vlan, formatted as <slot>.<port>.<vlan>. If the packet was received on an aggregation, the aggregation name is used in place of <slot>.<port>. • intid-string configured for the VLAN and port that the client-originated packet was received on. The intid-string is a variable length string of up to 64 characters.
remote-id-type	Used by the DHCPv6 server when assigning IP addresses. If the remote-id-option is enabled, LDRA includes this option on client-originated frames that have not already been relayed (not relay-forward messages). The remote-id option (option 37) identifies the LDRA device. The value used must be unique in the network. Valid values are: • device mac address, where the address is converted to a string of 12 hexadecimal digits • device hostname • rid-string, where the rid-string is configured for the VLAN and port that the client-originated packet was received on. The rid-string is a variable length string of up to 64 characters.
remote-id-enterprise-number	Specifies the enterprise number used in the remote-id option.
remote-id-option	Indicates whether to include the remote-id option in relay-forward messages.

LDRA examines DHCPv6 frames sent to UDP port 547 and applies rules based on the DHCPv6 message type, content, and settings of the port that the frame was received on. Port trust mode indicates whether a port or group of ports can be trusted when analyzing the DHCPv6 messages. A list of client ports and a list of server ports can be configured manually.

This table lists LDRA trust modes.

Table 3-7
LDRA trust modes

Trust mode	Description
untrusted	Client DHCP messages that have not been relayed, that is, are not relay-forward messages, are relayed to the server ports. Relay-forward client messages are dropped. Server DHCP messages are dropped. LDRA only intercepts server DHCP messages sent to port 547, which is the server/relay port. The relay does not intercept messages directly from the DHCP server to a client. For virtual switch relays, MPLS-VC interfaces cannot be defined as client.
client-trusted	Client DHCP messages are relayed, including relay-forward messages, that is, client messages that have already passed through a relay. Server DHCP messages are dropped. For virtual switch relays, MPLS-VC interfaces cannot be defined as client-trusted.
server-trusted	Server DHCP messages of type relay-reply are relayed toward the client. Client DHCP messages and server DHCP messages sent to the relay that are not of type relay-reply are dropped.
dualrole-trusted	For client DHCP messages, dualrole trusted mode functions the same as client-trusted mode. For server DHCP messages, dualrole trusted mode functions as a server-trusted mode. For virtual switch relays, MPLS-VC interfaces cannot be defined as dualrole-trusted.

These rules are enforced on DHCPv6 frames received on VLANs that have LDRA enabled:

- On client interfaces, intercept DHCPv6 messages directed to server (udp port 547) and addressed to ALL_DHCP_Relay_Agents_and_Servers (FF02::1:2). Drop any messages of type Advertise, Reply, Reconfigure, or Relay Reply.
- On client interfaces, intercept DHCPv6 messages directed to server (udp port 547) and addressed to ALL_DHCP_Relay_Agents_and_Servers (FF02::1:2). Drop Relay Forward messages received on non-trusted client ports.
- On client interfaces, intercept DHCPv6 messages directed to server (udp port 547) and addressed to ALL_DHCP_Relay_Agents_and_Servers (FF02::1:2). Drop all messages where hop count is greater than or equal to the hop count limit.

- On client interfaces, intercept DHCPv6 messages directed to server (udp port 547) and addressed to ALL_DHCP_Relay_Agents_and_Servers (FF02::1:2). Relay only on ports defined as server-trusted ports.
- On server-trusted ports, intercept DHCPv6 messages with UDP port 547 and link-local scoped source and destination IP addresses. Drop all messages that are not of type Relay Reply.
- On server-trusted ports, intercept DHCPv6 messages with UDP port 547 and link-local scoped source and destination IP addresses. Forward only on the interface identified in the interface-ID option of the Relay Reply message.

Procedures for LDRA are:

- "Configuring LDRA" on page 3-49
- "Displaying and clearing relay agent statistics" on page 3-57
- "Displaying LDRA information" on page 3-60

CVID bundling

DHCP relay over MPLS virtual switch with CVID bundling is not supported. The recommendations for DHCP relay over virtual switch are:

- The MPLS virtual switch must have only EVPLs with CVID bundling.
- All AC members/UNI ports must have ingress POP and egress PUSH transformations.
- DHCP relay always send packets to the server-trusted interfaces as untagged packets encapsulated in the MPLS frame.

If CVID bundling is configured

- Ingress action on the AC/UNI is still POP.
- On egress, on the AC/UNI, if the encapsulated packet from the MPLS VC is tagged, it may not be sent to the client.

If transforms are not configured, DHCP relay on MPLS VS still sends the DHCP packets to the server-trusted interfaces as untagged encapsulated packets in the MPLS frame.

DHCP relay limitations

The limitations pertaining to MPLS virtual switch DHCP relays are:

- MPLS VS DHCP relays require IGMP configuration meaning attachment circuits are configured with ingress-l2-transform pop and egress-l2-transform push. MPLS encapsulated traffic must not have a VLAN tag. If not configured correctly, traffic may not flow correctly.
- MPLS virtual circuits cannot be used to ingress DHCP relay client traffic.
- MPLS relay is only supported on VPLS VS and not VPWs and PBT. The VS cannot include sub-ports.

- Using DHCP relay with MPLS VS requires four classifier resources from transport-oam (total, not per-relay). If the classifier resources are not available, you cannot enable the MPLS VS relays.

General considerations for DHCP relay are:

- Untrusted interfaces accept DHCP client traffic. Previously, the interface had to be trust-type client (LDRA) or client-trusted (L2) to accept DHCP client traffic. This change conforms to the DHCP relay RFCs and brings consistency between L2 and LDRA relays.
- Any software-based relay processing can have substantial impact on the switch performance. CPU rate limiting for DHCP is advised when using DHCP relay.
- VLAN DHCP relay is not supported on cross-connected VLAN.
- DHCP relay support varies based on platform.

L3 DHCP relay agent

This section describes the major features supported by the l3 DHCP relay agent and provides a detailed description of what they mean and what user interfaces are provided for this feature.

The l3 DHCP relay agent is required in a multi-subnet environment where a DHCP client and a DHCP server reside in different subnets. Generally, DHCP messages are broadcast. For the messages to be exchanged between a DHCP client (PC) and DHCP server, both the client and server have to reside on the same subnet. This is because routers do not forward any broadcast IP packet to other interfaces. Therefore, a broadcast DHCP packet sent by a DHCP client cannot be delivered to DHCP servers on different subnets through a router. This restriction requires all individual subnets to have their own DHCP server for DHCP operation, which is not practically feasible in network operators' networks or corporate computer networks (too many DHCP servers are required in the network). To address this problem, the concept of a DHCP relay agent has long been adopted. One of the main roles of a relay agent is to add information to the DHCP request that can be used by the DHCP server in assigning addresses. By enabling the DHCP relay feature on the router, a subscriber is identified by the router interface through which it connects to the network (rather than by its MAC address).

Supported platforms for the l3 DHCP relay agent include:.

Table 3-8
SAOS-supported platforms for the l3 DHCP relay agent

Platform	L3 DHCP relay agent
3903	VLAN
3904	VLAN
3905	VLAN
3906	VLAN
3926	VLAN
3928	VLAN
3942	VLAN
5142	VLAN
5160	VLAN

L3 relay agents are aware of the location of the DHCP server and alter the DHCP client packet's destination address to reflect that knowledge. The core function of the l3 DHCP relay agent is to convert a broadcast DHCP packet into a unicast one, and forward it to a DHCP server.

The l3 relay agent works as a BOOTP relay agent, relaying DHCP packets received on one network to a DHCP server located on a different network.

The l3 DHCP relay agent receives the DHCP request from the client and relays the received request to the configured server. The server can provide multiple options to the client in response to the DHCP request. These options are needed by the client for ZTP. The l3 DHCP relay forwards the request from client to server and vice versa.

The l3 DHCP relay agent feature encompasses two sub-features:

- DHCP option 82 (Remote ID and Circuit ID sub-options)
- Interface trust modes

Option 82 format

L3 DHCP relay agent option 82 is described in RFC 3046. L3 DHCP relay agent option 82 solves security issues that arise from DHCP client requests coming from untrusted sources including:

- DHCP IP exhaustion attacks.
- DHCP client identifier spoofing.

- DHCP MAC address spoofing.
- DHCP gateway address, that is, giaddr spoofing.
- DHCP denial of service attack.

L3 DHCP relay agent option 82 is a collection of sub-options, including those for remote ID and circuit ID. The l3 DHCP relay agent adds option 82 to the DHCP frame received from the DHCP client and sends the frame to the DHCP server. The DHCP server use these options to allocate the IP address to the client, copy the option in the reply message, and send the DHCP message back to the DHCP relay agent. The l3 DHCP relay agent uses option 82 to find the IP interface on which the message needs to be sent back to the client. The l3 DHCP relay agent strips option 82 before sending the DHCP frame to the DHCP client.

Remote Identifier sub-option

The l3 DHCP relay agent adds a remote identifier to option 82. The remote identifier cannot exceed 64 bytes in length and it must be globally unique. The remote identifier may be used by the DHCP server to allocate the IP address to the DHCP client. The remote identifier can be configured to use one of the following parameters:

- device-mac (default)
- device-hostname
- rid-string

Circuit Identifier sub-option

The l3 DHCP relay agent adds a circuit identifier to option 82. The circuit identifier cannot exceed 64 bytes in length. The circuit identifier is used by the l3 DHCP relay agent to identify the interface on which the DHCP reply from the DHCP server is to be forwarded. The circuit identifier can be configured to use one of the following parameters:

- interface name (default)
- interface index
- cid-string

Ciena supports three options for option 82 configuration:

1. On—If option 82 is configured as “On”:
   a. L3 DHCP relay adds its own option 82 to the DHCP packet, no matter what is being received.
   b. L3 DHCP relay always adds option 82 whether packets are received with or without option 82. In case we receive packet with option82, it will be replaced with our option82.
2. Off—If option 82 is configured as “Off”:
   a. L3 DHCP relay does not add/strip or replace option 82 from packet.

3 Replace—If option 82 is configured as “Replace”:

   a. If packets with option 82 are received, Ciena replaces the option 82 with its own.

   b. If packets without option 82 are received, the l3 DHCP relay does not add its option 82 to the packet. The packet is forwarded to the server without option 82.

Relay agent RFC 3046 specifies that a DHCP frame received from an untrusted interface with a gateway address set to zero and the DHCP relay agent option already set is dropped. But there can be l2 DHCP relays closer to the host, so if a DHCP frame is received from a trusted interface, l3 relay forwards the packet with or without changing the information in the option 82 field (depending on the option 82 configurations on the l3 relay agent) and sets the gateway address.

Users can configure whether the DHCP relay agent trusts traffic sources. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP relay agent filters messages from untrusted sources. In an enterprise network, a trusted source is a device that is under your administrative control. These devices include the switches, routers, and servers in the network. Any device beyond the firewall or outside the network is an untrusted source.

Generally, host ports are treated as untrusted sources. In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

DHCP relay agent configurable interface trust modes

Users can configure “Untrusted” and “Trusted” trust modes. When an IP interface is attached to the DHCP instance, all the ports related to the IP interface are configured as “Ignore” ports. This is the default trust mode of interface and VLAN/port. Differences are:

- Untrusted—Client DHCP frames received on an untrusted interface without the DHCP relay option are forwarded to all the DHCP servers. Client DHCP frames received from an untrusted interface with the relay option already set are discarded.
- Trusted—Client DHCP frames and relayed client DHCP frames (that is, frames with option 82) are forwarded to all the trusted DHCP servers.

If an l3 DHCP relay agent receives an already relayed DHCP frame with the gateway address set and the gateway address matches any of the gateway addresses on the l3 relay agent, the DHCP frame is dropped.

If the gateway address in the packet does not match any of the gateway addresses on the l3 relay agent, the packet is forwarded to the server without changing the gateway address. In this case, a reply is directly sent to relay, which sets the gateway address.

To set the trust mode, there are three types of trust level provided to users:

- Interface/VLAN/port
- Interface level
- Instance level

By default, all interfaces are Ignore. If users configure trust levels on an instance, this means all the interfaces and their underlying VLAN/port associations are updated as per the trust setting on that instance.

This trust setting on a specific interface can be changed by changing the trust level of that specific interface. By changing the interface trust level, all VLAN/ port trust settings are updated as configured on the interface.

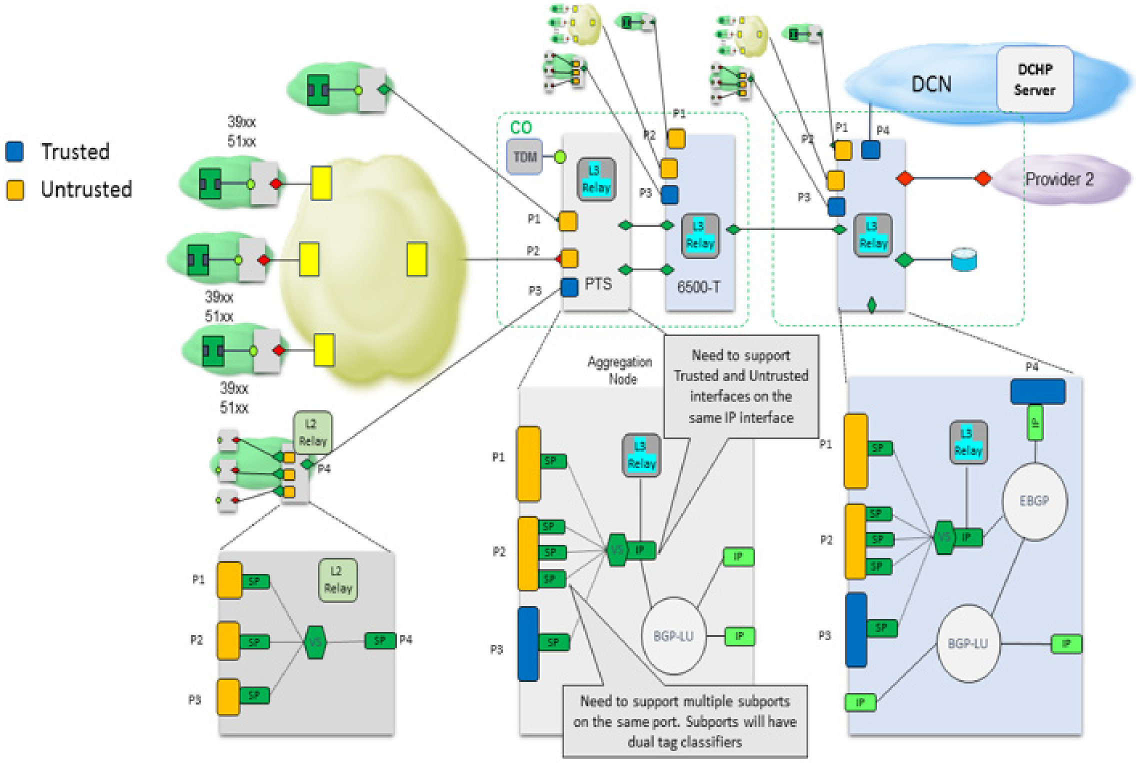
The third level of trust setting is VLAN/port of a specific interface, which users can override.

Trust levels are configured on the interface or instance by using the trust setting of VLAN/port of that interface.

Customer use case

In the following customer use case scenario, 39xx and 51xx work as DHCP clients while the Policy Traffic Switch (PTS) box is configured as the l3 relay. Initially, when users deploy 39xx or 51xx switches in the network, the DHCP request is transmitted on VLAN 127 and the PTS l3 relay is configured on VLAN 127 to process the DHCP request and forward it to the DHCP server.

Figure 3-3
Customer use case scenario



Limitations

1 The Internet Systems Consortium (ISC) DHCP relay process is restarted whenever there is a change in the DHCP relay configuration. This restart might lead to some packets being dropped whenever there is a race between configuration being applied on the relay and request/response packets being received on the relay agent. However, this drop might not impact the functionality because the client automatically performs a retransmission of each such request on a timely basis if the response for the previous one was not received. This drop might not be accounted for in drop statistics, as well, because Ciena maintains the statistics in the control plane (CP) and not in the data plane (DP).

2 Since the Internet Protocol (IP) interface cannot bind to the system management VLAN (default is 127), Ciena cannot configure the IP on the VLAN acting as the management VLAN. Users need to make sure that the VLAN used in the client is *not* used in the management VLAN on the relay agent to make it part of the relay process. Therefore, it is expected that the l3 DHCP relay device moves to a different management VLAN other than 127 for it to support zero touch provisioning (ZTP) operations for various clients on the access side.

Dependencies

1 The Internet Systems Consortium (ISC) DHCP relay package is part of the system. Currently, Ciena uses the ISC version “dhcp-4.1-ESV-R13”.

2 ISC DHCP relay is part of the binary loaded in DUT.

3 DHCP packets are trapped to the CPU based on UDP port 67/68. The trap is the same as in the l2 DHCP relay.

Debugging/logging

Logging is provided for the l3 DHCP relay feature. Users can set the diff-2 logging level. As of now, this logging level is provided for the user to configure.

```
+---- DHCP LOGGING DEBUG CONTEXT ---+
| State       | disabled         |     |
+-------------+-----------------+-----+
| Categories  | error            | Off |
|             | info             | Off |
|             | timers           | Off |
+------------+-----------------+-----+
```

Users can dump all the information related to l3 relay in system-dump. Information includes the l3 relay database maintained by the l3 relay manager. “Dhcp_l3_relay_debug.txt” is added to the system dump for debug purposes.

Procedures for l3 DHCP relay are:

- “Configuring global l3 DHCP relay agent instances” on page 3-66
- “Configuring interface-level l3 DHCP relay agent instances” on page 3-70

Network Time Protocol

With the Network Time Protocol (NTP) client, you can configure a device to automatically synchronize its time and date to a remote NTP server running Coordinated Universal Time (UTC). By default, the NTP client is enabled in polling mode without any configured servers. You can add servers manually or through DHCP. When the NTP client is enabled, date and time configuration received from an NTP server overrides any values manually set on the device.

NTP client supports authentication as per RFC 1305. By default, authentication is disabled. The network operator can configure either MD5 or SHA1 keys for authentication while in polling and broadcast modes. When authentication is enabled and packets are transmitted and received, they are only accepted if the message authentication code matches.

NTP servers configured via DHCP option 42 or DHCPv6 option 56 do not support authentication configuration.

Keys and related information are contained in a keys file. Each line of the keys file consists of a key ID in the range of 1 to 65,534 inclusive, a key type and a message digest key consisting of a printable ASCII string less than 40 characters, or a 40-character hexadecimal digit string. The string is entered using NTP authentication. For procedures, see "Configuring NTP authentication" on page 3-80.

The modes in which the NTP client operates are:

- polling (IPv4 and IPv6)
- broadcast (IPv4 only)
- multicast (IPv6 only)

The default mode is polling.

Changes to the NTP mode take effect immediately as long as NTP client is enabled.

Polling is the default mode so that the device can use NTP servers configured by means of DHCP option 42 or DHCPv6 option 56.

NTP servers can be configured by means of DHCP or DHCPv6, or manually configured by means of the CLI or SNMP. DHCP-configured servers override any user configured servers, that is, makes them operationally disabled. 39XX/51XX switches support up to 10 user-configured NTP servers or 20 DHCP/DHCPv6-configured servers, that is, 10 for DHCP and 10 for DHCPv6. When configuring NTP servers by means of DHCP or DHCPv6 hostnames are not currently supported.

In polling mode (default), the network operator must specify the hostnames (manual only) or IP addresses of NTP servers. The network operator can also specify the polling interval which indicates the time interval to request time information from the servers. One polling interval is used for all configured NTP servers.

Typically the polling interval is entered as a power of 2. The NTP client accepts 2^4(16 seconds) to 2^12(4096 seconds). Values of 16, 32, 64, 128, 256, 512, 1024, 2048, 4096 are accepted by the CLI. While NTP can support longer polling intervals, the NTP client on 39XX/51XX switches limits the range to maintain accuracy.

The network operator can also specify a minimum and maximum polling interval. By default, the minimum polling interval and maximum polling interval are set to 16 seconds. The minimum polling interval is used when the NTP client is not synchronized. The maximum polling interval is used after the client has synchronized to a server. This allows the NTP client to synchronize faster on bootup and then fall back to a longer polling interval once the NTP client has synchronized the clock.

The network operator can configure a notification for when the NTP client has synchronized its clock. This notification is provided in the form of an SNMP trap, an event that can be logged, and an outgoing syslog message.

In broadcast mode, the NTP client is not configured to use a specific server. Instead, the NTP client waits for broadcast servers on the same subnet to broadcast their current time. When the NTP client receives the first message, it interacts with that server to retrieve reliable time. When additional broadcast messages are received from that server, the NTP client calculates the time difference and adjusts the clock accordingly. If broadcast messages are received from several broadcast servers, the client selects the most accurate server to use.

NTP servers must be of version NTPv4 to support IPv6 multicast. The NTP client in multicast mode supports servers in the range of FF0X:0:0:0:0:0:0;101. NTP running over IPv6 uses multicast messages to send and receive clock updates instead of the IPv4 broadcast messages.

> ***Note:*** NTP servers synchronize with IPv4 broadcast servers when NTP client mode is set to multicast for IPv6. In multicast mode, SAOS can synchronize with IPv6 and IPv4 using broadcast traffic. The NTP client synchronizes with the available time, either IPv4 or IPv6.

The NTP drift file stores how far the local clock is out of synchronization with the NTP server. The NTP drift file is persistent upon re-boot. The NTP client checks the drift file, and if the drift is more than 128 ms, the local clock is updated. If the drift file information is inaccurate, for example, the device time does not synchronize correctly with the NTP server or exceeds a specified value, the drift file can be cleared and the NTP client can be restarted to force it to resynchronize with the server. When the drift file is cleared, a system event is logged.

NTP authentication support

NTP authentication support allows the NTP client to verify that the server is known and trusted. NTP supports these types of authentication:

- Message Digest 5 (MD5) — a private key called key-MD5. MD-5 is no longer considered secure.
- Secure Hash Algorithm (SHA)-1 — produces a 160-bit (20-byte) hash value which is usually rendered as a hexadecimal number 40 digits long.

The network operator can configure authentication for the NTP client to prevent an unwanted network intruder from masquerading as an NTP server. Authentication provides a way for the NTP client to verify that a server is a known and trusted NTP source. NTP authentication keys are codes that are encrypted on both the server and client and are used to identify the NTP time server. Each authentication key consists of a key ID and the key itself. Authentication works with both polling and broadcast modes.

> ***Note:*** Authentication is not supported for NTP servers configured with DHCP option 42. When the NTP servers are configured with DHCP, any user configured NTP settings are overridden.

The authentication key number acts as a reference to the specified authentication key. The actual keys must be identical on both the NTP client and the NTP server. The client can use a subset of the authentication keys specified on the NTP server, and the keys are case sensitive. Authentication is supported in both polling and broadcast modes.

In polling mode, the NTP client configuration must specify the association of the key number to a server. When configured, the NTP client sends a request for time to the NTP server with corresponding key and authentication code. The NTP server, after validating the client's authentication, replies with an encrypted response along with timestamp information. Upon receipt of the timestamp, the NTP client validates the server's authentication. If valid, the time configuration is updated, otherwise, the time configuration is rejected. Authentication can be enabled on the system, but if the user has specified NTP_N)_KEY as the key, then no authentication is performed.

In broadcast mode, since the server is auto-detected by the client, association of the key number to a server cannot be configured at the client. However the corresponding key number and key values must be configured at the client. The NTP server broadcasts timestamp information along with the key number and authentication code encoded in the packet. Upon receipt of the timestamp, the NTP client decrypts the key and verifies it against a list of trusted keys. If the key matches a trusted key, the NTP client starts synchronizing with that NTP server using the same key number and authentication code as the server.

Procedures for NTP are:

- “Configuring NTP” on page 3-74
- “Configuring NTP servers” on page 3-76
- “Adding NTP servers to the NTP client server list” on page 3-78
- “Configuring NTP authentication” on page 3-80
- “Clearing the drift file” on page 3-85

- “Displaying NTP state and configured servers” on page 3-86

Neighbor Discovery Protocol

The Neighbor Discovery Protocol uses a neighbor discovery cache database as new neighbor addresses are advertised to the node. Similar to ARP, a MAC to IPv6 address mapping is kept for a limited time. NDP is enabled while IPv6 is enabled.

The neighbor discovery cache entries are entered and no static configuration is supported for local and remote interfaces. The network operator can display the contents of the cache and clear all entries in the cache to allow new entries to be populated.

Neighbor discovery is an enhancement in ICMPv6 that performs these functions:

- autoconfigures IPv6 addresses
- determines network prefixes, routes and other config information
- performs duplicate IP address detection (DAD)
- determines L2 addresses of nodes on the same link
- finds neighboring routers that can forward packets
- tracks which neighbors are reachable and which are not (NUD)
- detects changes in link-layer addresses

The neighbor and destination caches, maintained by IPv6 nodes, are similar to the ARP table cache.

The neighbor cache maintains a list of neighbors shown by their unicast address along with information about the neighbor link-layer address, a flag indicating whether it is a router or a host, reachability status and other relevant information.

The destination cache maintains information about destinations to which traffic has been sent recently including remote and local destinations. The neighbor cache is a subset of the destination cache. It also contains information about MTU sizes and round trip times.

Procedure 3-1
Configuring the serial console port

The serial console port is enabled by default.

Disable the serial console port when you do not want to allow access to a PC or terminal server.

Configuring the serial console port comprises these tasks:

- enabling the serial console port
- disabling the serial console port
- displaying information for the serial console port

Step **Action**

To enable the serial console port

1 Enable the serial console port:

```
interface serial-console enable
```

To disable the serial console port

2 Disable the serial console port:

```
interface serial-console disable
```

To display information for the serial console port

3 Display information for the serial console port:

```
interface serial-console show
```

—end—

Procedure 3-2
Configuring Telnet

By default, the Telnet server is enabled and supports 15 simultaneous sessions by default. These sessions are shared with SSH. You can adjust the number of allowed connections per user to ensure proper management and usage of the device.

Disable Telnet if you want to use SSH exclusively.

The network operator can

- enable Telnet
- disable Telnet
- display Telnet server configuration information

Step **Action**

To enable Telnet

1 Enable Telnet:

```
telnet server enable
```

To disable Telnet

2 Disable Telnet:

```
telnet server disable
```

To display Telnet server configuration information

3 Display Telnet server configuration information:

```
telnet server show
```

—end—

Example

This example shows the output for the telnet server show command.

```
              > telnet server show

+--- TELNET GLOBAL CONFIGURATION ---+
| Parameter         | Value         |
+-------------------+---------------+
| Server            | Enabled       |
| Dos Max Attempts  | 15            |
+-------------------+---------------+

+------- TELNET GLOBAL STATUS ------+
| Attribute             | Value     |
+-----------------------+-----------+
| Active Limited Users  | 0         |
| Active Admin Users    | 0         |
| Active Super Users   | 1          |
| Active Diag Users    | 0          |
| Total Active Users   | 1          |
+----------------------+------------+
```

Procedure 3-3
Configuring the Telnet DoS protection limit

You can configure the Telnet DoS protection limit when you want to enforce a limit other than the default of 15.

Step **Action**

To configure Telnet DoS protection limit

1 Configure Telnet Dos protection limit:

```
telnet server set dos-max-attempts <Number: 1...60>
```

> ***Note:*** This is applicable for IPv4 and IPv6 both. On execution of the command, similar protection limit as mentioned in the CLI, will be set for IPv6 and IPv4. For example, if limit is configured to maximum 60, it allows 60 telnet connections for IPv4 and 60 for IPv6, separately. However, it is recommended to create maximum supported telnet connections including both IPv4 and IPv6.

To reset Telnet DoS protection limit to the default of 15

2 Reset Telnet Dos protection limit to the default of 15:

```
telnet server unset dos-max-attempts
```

To display Telnet server configuration information

3 Display Telnet server configuration information:

```
telnet server show
```

—end—

Example

This example sets the Telnet DoS protection limit to 20.

```
> telnet server set dos-max-attempts 20
```

The following sample output shows that the limit is set to 20.

```
>telnet server show
```

```
+--- TELNET GLOBAL CONFIGURATION ---+
| Parameter         | Value         |
+-------------------+---------------+
| Server            | Enabled       |
| Dos Max Attempts  | 20            |
+-------------------+---------------+
```

The following command restores the limit to the default of 15.

```
>telnet server unset dos-max-attempts
```

The following sample output shows that the limit is now set to 15.

```
>telnet server show
```

```
+--- TELNET GLOBAL CONFIGURATION ---+
| Parameter         | Value         |
+-------------------+---------------+
| Server            | Enabled       |
| Dos Max Attempts  | 15            |
+-------------------+---------------+
```

Procedure 3-4
Running the Telnet client

Run the Telnet client to establish a Telnet connection to other Telnet servers.

Step **Action**

1 Run the Telnet client:

```
telnet client connect ip <IpHost> [-l <UserName>]
{<IpAddress>} [<port>]
```

where

[-l <UserName>] Logs in with the specified user. If left unspecified, the remote system prompts for the user name.

<IpAddress> is IP address to Telnet to.

<port> is the TCP port. By default, the port is 23.

—end—

Example

This example shows sample output for the telnet command.

```
> telnet 10.10.121.19

Entering character mode
Escape character is '^]'.

3942 00:02:A1:24:0E:30
SAOS is True Carrier Ethernet TM software.

3942 login: su
Password:

SAOS is True Carrier Ethernet TM software.

Welcome to the shell.
> exit

Goodbye.
```

Procedure 3-5
Telneting to another system using Telnet client

Telnet to another system using Telnet client.

Step **Action**

1 Telnet to another system:

```
telnet client connect <ip-host-object>]
```

where

<ip-host-object> is the IP address of the system you are telneting to.

—end—

Procedure 3-6
Configuring DHCP client

Supported DHCP operations include:

- setting DHCP options
- enabling the DHCP client
- disabling the DHCP client
- renewing the leased IP address
- setting the interface and discovery interval
- displaying the current DHCP configuration

The DHCP client is enabled by default for low-touch provisioning. For more information, refer to the *Hardware Installation Manual* for the device. Note that this information only applies to IPv4.

The DHCP client supports the DHCP options summarized in the Supported DHCP Options table. A complete list of DHCP options is defined in RFC 1533.

Table 3-9
Supported DHCP Options

Option #	Name	Description
1	subnet	Specifies the subnet mask for the interface. Default is on.
2	time-offset	Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). Default is on.
3	router	Specifies a list of IP addresses for routers on the client's subnet (gateways). Routers should be listed in order of preference. Default is on.
6	dns	Specifies a list of five Domain Name System (STD 13, RFC 1035 [8]) name servers available to the client. Servers should be listed in order of preference. Default is on.
7	log-server	Specifies a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference. Used by Syslog. Note that this DHCP option provides no mechanism to configure the UDP port for a syslog server. Any syslog servers configured by DHCP use the default UDP port for syslog. Default is on.
12	host-name	Specifies the name of the client. The name may or may not be qualified with the local domain name. Default is on.
15	domain-name	Specifies the domain name that the client can use when resolving host names via the Domain Name System (DNS). Default is on.
42	ntp	Specifies a list of IP addresses indicating Network Time Protocol (NTP) [18] servers available to the client. Servers should be listed in order of preference. Default is on.
51	lease-time	Requests the lease time for the IP address. The default client lease-time is 1 hour and the default for this option is off.

Table 3-9
Supported DHCP Options (continued)

Option #	Name	Description
66	tftp-server	The TFTP address is only used to retrieve the command file and then is discarded. Default is on. If Option 66 is received in the DHCP reply and the option is On, then that IP address is used for the TFTP server, otherwise the value in 'siaddr' is used.
67	boot-file	Specifies to use the boot image specified by the DHCP server.
125	vendor-identifying, vendor specific information	Specifies Secure Zero Touch Provisioning (SZTP). A security license and SFTP credentials must be factory pre-installed to use SZTP. This option takes precedence over options 66 and 67 if it is enabled and the security license and SFTP credentials (encrypted username and password) are pre-installed. The username and password can be changed via the CLI. For more information about SZTP, refer to *39XX/51XX Switches and Platforms Base Configuration.*

Step **Action**

To set DHCP options

1 Set DHCP options:

```
dhcp client options set [subnet <on|off>] [time-offset
<on|off>] [ntp <on|off>] [router <on|off>] [dns <on|off>]
[log-server <on|off>] [host-name <on|off>] [domain-name
<on|off>] [ntp <on|off>] [lease-time <on|off>] [tftp-
server <on|off>] [boot-file <on|off>] [vivsi <on|off>]
```

where

[subnet <on|off>]	is the subnet DHCP option.
[time-offset <on|off>]	is the time offset DHCP option.
[ntp <on}off>]	is the NTP DHCP option.
[router <on|off>]	is the router DHCP option.
[dns <on|off>]	is the DNS DHCP option.
[log-server <on|off>]	is the log server DHCP option.
[host-name <on|off>]	is the host name DHCP option.
[domain-name <on|off>]	is the domain name DHCP option.

where

[ntp <on|off>]	is the NTP DHCP option.
[lease-time <on|off>]	is the lease time option.
[tftp-server <on|off>]	is the TFTP server DHCP option.
[boot-file <on|off>]	is the boot file DHCP option.
[vivsi <on|off>]	is the VIVSI DHCP option.

To enable the DHCP client

2 Enable the DHCP client:

```
dhcp client enable
```

To disable the DHCP client

3 Disable the DHCP client:

```
dhcp client disable
```

To renew the leased IP address

4 Renew the leased IP address:

```
dhcp client lease renew
```

To set the interface and discovery interval

5 Set the interface and discovery interval:

```
dhcp client set {[interface <local | remote>, [discovery-
interval <NUMBER: 1-60>]}
```

where

[interface <local | remote>]	is the interface on which to run DHCP.
[discovery-interval <NUMBER: 1-60>]	is the DHCP discovery interval in seconds.

To display the DHCP configuration

6 Display the current DHCP configuration:

```
dhcp client show
```

—end—

Example

This example shows sample output for the dhcp client show command.

```
> dhcp client show
```

```
+-------------------- DHCP CLIENT STATE ---------------------+
| Parameter                            | Value               |
+--------------------------------------+---------------------+
| Interface Name                       | tap1                |
| Admin State                          | Enabled             |
| Oper State                           | Enabled             |
| DHCP State                           | Disabled            |
| Discovery Interval                   | 30                  |
| Lease Time (days hh:mm:ss)           | 0:00:00:00          |
| Lease Remaining (seconds)            | 0                   |
| Renewal (T1) Time (seconds)          | 0                   |
| Rebinding (T2) Time (seconds)        | 0                   |
| DHCP Server                          | 0.0.0.0             |
+--------------------------------------+---------------------+
```

```
+-------------------------- DHCP/BOOTP OPTIONS STATE --------------------------+
| Option | Description                 | State | Value                          |
+--------+-----------------------------+-------+--------------------------------+
| 1      | Subnet Mask Option          |  On   |                                |
| 2      | Time Offset Option          |  On   |                                |
| 3      | Router Option               |  On   |                                |
| 6      | Domain Name Server Option   |  On   |                                |
| 7      | Log Server Option           |  On   |                                |
| 12     | Host Name Option            |  On   |                                |
| 15     | Domain Name Option          |  On   |                                |
| 42     | NTP Servers Option          |  On   |                                |
| 51     | Lease Time Option           |  Off  |                                |
| 66     | Tftp Server Name Option     |  On   |                                |
| 67     | Bootfile Name Option        |  On   |                                |
| 125    | V-I Vendor-Specific Info    |  On   |                                |
+--------+-----------------------------+-------+--------------------------------+
```

Procedure 3-7
Configuring the DHCPv6 client

Configure the DHCPv6 client according to network requirements.

You can

- clear DHCPv6 client statistics
- globally disable DHCPv6 client
- globally enable DHCPv6 client
- renew client lease
- set DHCPv6 client parameters
- set attributes back to default values

Step **Action**

To clear DHCPv6 client statistics

1 Clear DHCPv6 client statistics:

```
dhcpv6 client clear statistics
```

To globally disable DHCPv6 client

2 Globally disable DHCPv6 client:

```
dhcpv6 client disable
```

To globally enable DHCPv6 client

3 Globally enable DHCPv6 client:

```
dhcp v6 client enable
```

To renew client lease

4 Renew client lease:

```
dhcpv6 client lease renew
```

To set DHCPv6 client parameters

5 Set DHCPv6 client parameters:

```
dhcpv6 client set {[interface <local | remote>]
[preferred-lifetime <SECONDS: 0..MAX>] [valid-lifetime
<SECONDS: 0..MAX>]}
```

where

interface <local | remote>	Indicates whether the interface is local or remote. The default value is remote.
preferred-lifetime <SECONDS: 0..MAX>	is the preferred lifetime. The default value is 0.
valid-lifetime <SECONDS: 0..MAX>	is the valid lifetime. The default value is 0.

To set attributes back to default values

6 Set attributes back to default values:

```
dhcpv6 client unset {[interface] [preferred-lifetime]
[valid-lifetime]}
```

where

interface <local | remote>	Indicates whether the interface is local or remote. The default value is remote.
preferred-lifetime <SECONDS: 0..MAX>	is the preferred lifetime. The default value is 0.
valid-lifetime <SECONDS: 0..MAX>	is the valid lifetime. The default value is 0.

—end—

Procedure 3-8
Configuring DHCPv6 client options

Configuring DHCPv6 client options to request network configuration includes these tasks:

- setting the DHCPv6 client options to request
- setting the DHCPv6 client options to default values

Step **Action**

To set the DHCPv6 client options to request

1 Set the DHCPv6 client options to request and to use if received in a DHCPv6 INFORMATION_REPLY or REPLY message:

```
dhcpv6 client options set {[bootfile-url <on|off>] [dns-
servers <on|off>] [domain-list <on|off>] [ntp-servers
<on|off>] [posix-timezone <on|off>] [tzdb-timezone
<on|off>]}
```

where

bootfile-url <on|off> is the URL to the bootfile. The default value is on.

dns-servers <on|off> is the DNS server. The default value is on.

domain-list <on|off> is the domain list. The default value is on.

ntp-servers <on|off> is the NTP server. The default value is on.

posix-timezone <on|off> is the POSIX TZ string. The default value is on.

tzdb-timezone <on|off> is the timezone database. The default value is on.

To set DHCPv6 client options to default values

2 Set the DHCPv6 client options to default values:

```
dhcpv6 client options unset {[bootfile-url] [dns-servers]
[domain-list <on|off>] [ntp-servers] [posix-timezone]
[tzbd-timezone]}
```

—end—

Procedure 3-9
Enabling DHCPv6 client rapid commit

DHCPv6 rapid client commit uses two messages: SOLICIT and REPLY.

You can

- enable DHCPv6 client rapid commit
- disable DHCPv6 client rapid commit

Step	Action

To enable DHCPv6 client rapid commit

1 Enable rapid commit functionality

```
dhcpv6 client rapid-commit enable
```

To disable DHCPv6 client rapid commit

2 Disable rapid commit functionality

```
dhcpv6 client rapid-commit disable
```

—end—

Procedure 3-10
Displaying DHCPv6 client information

Display DHCPv6 client information to determine current configuration.

DHCPv6's Option 42 named time zones may not appear to work right in all circumstances. This is because SAOS does not support named zones, which contain rules about daylight savings time (DST). At the time of the lease SAOS converts the named zone to a fixed time-offset. If a DST change occurs after this, the time-offset appears to be an hour (usually) off until the lease is refreshed and Option 42 is re-processed.

You can display

- client state
- option configuration
- rapid commit settings

Step **Action**

To display DHCPv6 client state

1 Display DHCPv6 client state:

```
dhcpv6 client show [options] [state] [statistics]
```

where

options	displays DHCPv6 client option information
state	displays DHCPv6 client state
statistics	displays DHCPv6 client statistics.

To display DHCPv6 client rapid commit settings

2 Display DHCPv6 client rapid commit settings:

```
dhcpv6 client rapid-commit show
```

—end—

Example

This example shows sample output for the dhcpv6 client show command.

```
+---------------------------------- DHCPV6 CLIENT STATE --------------------+
|Parameter                                             | Value               |
+------------------------------------------------------+---------------------+
|Interface Name                                        | remote              |
|Admin State                                           | Enabled             |
|Rapid Commit State                                    | Enabled             |
|Requested Preferred Lifetime (days hh:mm:ss)          | 0 00:00:00          |
|Requested Valid Lifetime (days hh:mm:ss)              | 0 00:00:00          |
+------------------------------------------------------+---------------------+
|Oper State                                    | Enabled                             |
|DHCPv6 State                                  | Bound                               |
|Autoconfiguration State                       | Stateful                            |
|Router Advertisement Flags                    | M=1, O=0                            |
|Renewal Time (T1) (days hh:mm:ss)             | 0 00:02:30                          |
|Rebinding Time (T2) (days hh:mm:ss)           | 0 00:03:45                          |
|Preferred Lifetime (days hh:mm:ss)            | 0 00:03:07                          |
|Valid Lifetime (days hh:mm:ss)                | 0 00:05:00                          |
|Remaining Renewal Time (T1) (days hh:mm:ss)   | 0 00:02:27                          |
|Remaining Rebinding Time (T2) (days hh:mm:ss) | 0 00:03:42                          |
|Remaining Preferred Lifetime (days hh:mm:ss)  | 0 00:03:04                          |
|Remaining Valid Lifetime (days hh:mm:ss)      | 0 00:04:57                          |
|DHCPv6 Server Address                         | 2001:db8::1                         |
|DHCPv6 Server Identifier                      | 0:1:0:1:18:5b:71:7c:0:f:fe:7f:60:df|
|Elapsed Time                                  | 0.00 sec                            |
+----------------------------------------------+-------------------------------------+
```

```
+-------------------------- DHCPV6 OPTIONS STATE ----------------------------+
|Option| Description             |State| Value                                |
+------+-------------------------+-----+--------------------------------------+
|23    | DNS Server List Option|  On  | 2001:db8::                            |
|      |                       |      | 101::101                              |
|      |                       |      | 101::102                              |
|24    | Domain List Option    |  On  | ipv6.ciena.net.                       |
|41    | POSIX Timezone Option |  On  | PST8PDT7,M3.2.0/02:00,M11.1.0/02:00   |
|42    | TZDB Timezone Option  |  On  | Pacific/Honolulu                      |
|56    | NTP Servers Option    |  On  | 2001:db8::                            |
|...
|59    | Bootfile URL Option   |  On  | tftp://dtest.ipv6.ciena.net/le-lnx.xml|
+------+-----------------------+-----+---------------------------------------+
```

This example shows sample output for the dhcpv6 client rapid-commit show command.

```
+--------------- DHCPV6 RAPID COMMIT STATE -----------------+
| Parameter                          | Value                |
+------------------------------------+----------------------+
| Interface Name                     | remote               |
| Admin State                        | Enabled              |
| Oper State                         | Enabled              |
| DHCPv6 State                       | Bound                |
| Rapid Commit State                 | Enabled              |
+------------------------------------+----------------------+
```

Procedure 3-11
Configuring the L2 DHCP relay agent

Configure the L2 DHCP relay agent to forward DHCP requests and replies. L2 DHCP can be configured based on a VLAN membership, Q-in-Q or MPLS virtual circuit. For a virtual switch relay, vs-port is the Q-in-Q subscriber member/MPLS access circuit (AC). The setting applies to the specified port and optional VLAN if using an EVPL. For an MPLS virtual switch, the mpls-vc setting applies to the specified MPLS virtual circuit (VC).

Circuit ID and remote ID are associated with ports configured with trust type client-trusted or dual-role trusted. Circuit ID and remote ID cannot be set for an MPLS VC. For an MPLS VC, the trust type can only be server trusted or untrusted.

When a client message is relayed, the ingress client port configuration is used to provide the circuit ID and remote ID information. When the relay receives a server response message that contains relay information, the relay collects circuit ID and remote ID information from the relay portion of the message and uses the circuit ID and remote ID information to look up client ports.

The circuit ID information is the primary identification of the client port. As such, when using a circuit-id-type of cid-string, the string values must be unique for each circuit in the relay.

> ***Note 1:*** DHCP relay agent can be enabled or disabled on a VLAN or virtual switch. See Table 3-2.
>
> ***Note 2:*** If an L2 DHCP relay agent is created but not enabled for a VLAN, and that VLAN is then added to a virtual circuit, the L2 DHCP relay agent is created for the provider VLAN for Q-in-Q, and L2 DHCP relay is disabled for that VLAN. L2 DHCP relay cannot be enabled for the provider VLAN from the CLI.

Step **Action**

To configure L2 DHCP relay agent using a VLAN

1 Enable the L2 DHCP relay agent:

```
dhcp l2-relay-agent enable
```

2 Create the L2 DHCP relay agent for the selected VLAN:

```
dhcp l2-relay-agent create vlan <VLAN list>
```

3 Set the circuit ID type, remote ID type and replace-option82:

```
dhcp l2-relay-agent set [circuit-id-type {<slot-
port|slot-port-vlan|cid-string>] [remote-id-type
<device-mac|device-hostname|rid-string>][replace-
option82 on|off]}
```

where

circuit-id-type {<slot-port|slot-port-vlan|cid-string>]	sets the circuit-id-type
remote-id-type <device-mac|device-hostname|rid-string>]	sets the remote
replace-option82 on|off	sets the replace-option 82 on or off.

4 Set the VLAN and port attributes:

```
dhcp l2-relay-agent set vlan <vlan relay#> port <vlan
port> {[trust-mode <client-trusted|server-
trusted|dualrole-trusted| untrusted>] [cid-string
<String[64]>]} [rid-string <String[64]>]
```

where

vlan <vlan relay #>	is the VLAN relay number.
port <vlan port>	are the ports to set the attributes on.
[trust-mode <client-trusted | server-trusted | dualrole-trusted | untrusted>	sets the trust-level.
cid-string <String[64]>	sets the circuit ID string.
rid-string <String[64]>	sets the remote ID string.

5 Enable the L2 DHCP relay agent for the selected VLAN or VLANs:

```
dhcp l2-relay-agent enable vlan <VLAN list>
```

6 Confirm the configuration:

```
dhcp l2-relay-agent show
```

To configure L2 DHCP relay agent using a virtual switch

7 Enable the L2 DHCP relay agent:

```
dhcp l2-relay-agent enable
```

8 Create the L2 DHCP relay agent for the selected VLAN:

```
dhcp l2-relay-agent create vs-object-list>
```

9 Set the virtual switch and port attributes:

```
dhcp l2-relay-agent set vs-port <port-object-list> vs
<vs-object>[vlan <vlan>]{[trust-mode <client-
trusted|server-trusted|dualrole-trusted| untrusted>]
[cid-string <String[64]>]} [rid-string <String[64]>]
```

where

vs-port <port-object-list>	is the virtual switch that you are setting the port attributes on.
port <port-object-list>	are the ports to set the attributes on.
vs <vs-object>	is the virtual switch.
[trust-mode <client-trusted | server-trusted | dualrole-trusted | untrusted>	sets the trust-level.
cid-string <String[64]>	sets the circuit ID string.
rid-string <String[64]>	sets the remote ID string.

10 Enable the L2 DHCP relay agent for the selected virtual switch:

```
dhcp l2-relay-agent enable <vs-object-list>
```

11 Confirm the configuration:

```
dhcp l2-relay-agent show
```

To configure L2 DHCP relay agent using an MPLS virtual circuit

12 Enable the L2 DHCP relay agent:

```
dhcp l2-relay-agent enable
```

13 Set the MPLS-VC and trust mode:

```
dhcp l2-relay-agent set mpls-vc <vc-name> vs <vs-object-
list> trust-mode server-trusted
```

14 Confirm the configuration:

```
dhcp l2-relay-agent show
```

—end—

Examples

This example configures a VLAN on a Layer 2 DHCP relay agent.

```
dhcp l2-relay-agent enable
dhcp l2-relay-agent create vlan 111
dhcp l2-relay-agent set circuit-id-type cid-string
dhcp l2-relay-agent set vlan 111 port 10
trust-mode server-trusted
dhcp l2-relay-agent enable vlan 111
dhcp l2-relay-agent set vlan 111 port 1-3 trust-mode
client-trusted
dhcp l2-relay-agent set vlan 111 port 1 cid-string client1
dhcp l2-relay-agent set vlan 111 port 2 cid-string client2
dhcp l2-relay-agent set vlan 111 port 3 cid-string client3
```

This example configures a virtual switch on a Layer 2 DHCP relay agent with AC or port 1 on vlan 222 and a VC or primary VC.

```
dhcp l2-relay-agent enable
dhcp l2-relay-agent create vs relaymplsvs
dhcp l2-relay-agent set circuit-id-type cid-string
dhcp l2-relay-agent set vs-port 1 vs relaymplsvs vlan 222
trust-mode client-trusted cid-string mplsAC1
dhcp l2-relay-agent set mpls-vc primaryVC vs relaymplsvs
trust-mode server-trusted
dhcp l2-relay-agent enable relaymplsvs
```

This example shows sample output for the dhcp l2-relay-agent show command.

```
dhcp l2-relay-agent show
```

```
5142*> dhcp l2-relay-agent show

+---------- L2 GLOBAL SETTINGS ---------+
| Setting           | Value            |
+-------------------+-------------------+
| Global Admin      | Enabled           |
| Circuit ID Type   | CID-String        |
| Remote ID Type    | Hostname          |
| Replace Option82  | Off               |
+-------------------+-------------------+

+---------- L2 GLOBAL STATISTICS --------+
| Statistic          | Value             |
+--------------------+-------------------+
| Relayed            | 9                 |
| Dropped            | 6                 |
| Forwarded          | 0                 |
| Not For Relay      | 0                 |
+--------------------+-------------------+

+--------------- L2 RELAY AGENT STATE ------------------+
| VLAN ID |  VS Name        | Admin State | Oper State  |
+---------+-----------------+-------------+-------------+
| MPLS-1  | relaymplsvs     | Enabled     | Enabled     |
+---------+-----------------+-------------+-------------+
+------------------------ TRUSTED PORT SETTINGS ------------------------+
| VLAN     | Port          | SubVLAN | isActive        | Trust Mode      |
+----------+---------------+---------+-----------------+-----------------+
| MPLS-1   | primaryVC     |         | Active          | Server Trusted  |
| MPLS-1   | 1             |   222   | Active          | Client Trusted  |
+----------+---------------+---------+-----------------+-----------------+
+--------------------------- CID STRING SETTINGS ----------------------------+
| VLAN     | Port          | SubVLAN | Circuit ID String                      |
+---------+--------------+---------+-----------------------------------------+
| MPLS-1  |   1          |  222    | mplsAC1                                  |
+---------+--------------+---------+-----------------------------------------+
+--------------------------- RID STRING SETTINGS ----------------------------+
| VLAN     | Port          | SubVLAN | Remote ID String                       |
+---------+--------------+---------+-----------------------------------------+
| No RID String entries were found                                           |
+---------+--------------+---------+-----------------------------------------+
```

Procedure 3-12
Creating lists of trusted client ports and server ports

Create lists of trusted client ports and lists of trusted server ports to reduce DHCP broadcast traffic and spoofing attacks through the use of trusted ports. Use this procedure to create lists of trusted client ports and server ports for L2 DHCP relay agent and LDRA.

You can create lists of client ports and lists of server ports for:

- L2 DHCP relay agent
- LDRA

Step **Action**

To create lists of client ports and lists of server ports for L2 DHCP relay agent on a VLAN(s) or virtual switch

1 Set the VLAN or virtual switch and port attributes:

```
dhcp l2-relay-agent set vs-port <port-object-list> vs
<vs-object> [vlan <vlan>] {trust-mode <client-trusted |
server-trusted
```

To create lists of client ports and lists of server ports for LDRA on a VLAN(s) and virtual switch

2 Set the trust mode of LDRA on the virtual switch and VLAN and port:

```
dhcpv6 ldra set vs-port <port-object-list> vs <vs-object>
[vlan <vlan>] trust-mode client-trusted | server-trusted
```

—end—

Procedure 3-13
Configuring LDRA

Configure LDRA on a

- VLAN
- Q-in-Q virtual switch
- MPLS virtual circuit

Interface ID and remote ID are associated with ports configured with trust type client-trusted or dual-role trusted. When a client message is relayed, the client port is used to provide the interface ID and remote ID information (optional). The remote ID is controlled by the LDRA global config remote-id-option. When the relay receives a server response message that contains relay information, the relay collects interface ID and remote ID information from the relay portion of the message and uses the interface ID and remote ID information to look up client ports.

The interface ID information is the primary identification of the client port. The remote ID is not part of this process. As such, when using an interface-id-type of intid-string, the string values must be unique for each interface in the relay. For LDRA, the remote ID is passed toward the server if that option is enabled.

Step **Action**

To configure LDRA on a VLAN

1 Enable LDRA:

```
dhcpv6 ldra enable
```

2 Create LDRA for the specified VLAN(s) or virtual switch(es):

```
dhcpv6 ldra create vlan <VLAN>
```

3 Set LDRA attributes:

```
dhcpv6 ldra set {[interface-id-type {slot-port|slot-port-
vlan|intid-string}] [remote-id-type {device-mac|device-
hostname|rid-string}] [remote-id-enterprise-number
<enterprise-number>] [remote-id-option {on|off}]}
```

where

interface-id-type {slot-portl slot-port-vlanl intid-string}	is the value type for the interface-ID option of relay-forward messages. The default value is slot-port.
remote-id-type {device-macl device-hostnamelrid-string}	is the value type for the remote-id option of relay-forward messages. The default value is device-mac.
remote-id-enterprise-number <enterprise-number>	is the enterprise-number used in the remote-id option. Valid values are 1 to 4294967295. The default value is 3561, which is the Broadband Forum enterprise number. The Ciena enterprise number is 1271.
remote-id-option {onloff}	indicates whether to include the remote-id option in relay-forward messages. The default value is off.

4 Set the trust mode of LDRA on the VLAN and port:

```
dhcpv6 ldra set <vlan-object-list> <port-object-list>
trust-mode {client-trusted | server-trusted | dualrole-
trusted | untrusted}
```

where

<vlan>	is the VLAN.
port <port list>	is the port list.
trust-mode {client-trusted l server-trusted l dualrole-trusted l untrusted}	is the trust mode. For descriptions of trust modes, see Table 3-7.

5 Set the values for the interface-ID and remote ID for the VLAN or virtual switch and port:

```
dhcpv6 ldra set vlan <vlan> port <port list> {[intid-
string <interfaceID-string>] [rid-string <remoteID-
string>]}
```

where

vlan <VLAN>	is the VLAN.
port <port list>	is the port list.
intid-string <interfaceID-string>	is the value used for the interface-ID option for this VLAN and port. Valid values are 1 to 64.
rid-string <remoteID-string>	is the value used for the remote-ID option for this VLAN and port. Note that the remote-id-option must be enabled for this value to be included. Valid values are 1 to 64.

6 Enable LDRA for the specified VLAN or VLANs:

```
dhcpv6 ldra enable vlan <VLAN>
```

7 Confirm the configuration:

```
dhcpv6 ldra show vlan <VLAN>
```

where

vlan <VLAN>	is the VLAN that you want to view LDRA configuration for.

To configure LDRA on a Q-in-Q virtual switch

8 Enable LDRA:

```
dhcpv6 ldra enable
```

9 Create LDRA for the specified VLAN(s) or virtual switch(es):

```
dhcpv6 ldra create <vs-object>
```

10 Set LDRA attributes:

```
dhcpv6 ldra set {[interface-id-type {slot-port|slot-port-
vlan|intid-string}] [remote-id-type {device-mac|device-
hostname|rid-string}] [remote-id-enterprise-number
<enterprise-number>] [remote-id-option {on|off}]}
```

where

interface-id-type {slot-port| slot-port-vlan| intid-string}
is the value type for the interface-ID option of relay-forward messages. The default value is slot-port.

remote-id-type {device-mac| device-hostname|rid-string}
is the value type for the remote-id option of relay-forward messages. The default value is device-mac.

remote-id-enterprise-number <enterprise-number>
is the enterprise-number used in the remote-id option. Valid values are 1 to 4294967295. The default value is 3561, which is the Broadband Forum enterprise number. The Ciena enterprise number is 1271.

remote-id-option {on|off}
indicates whether to include the remote-id option in relay-forward messages. The default value is off.

11 Set the trust mode of LDRA on the Q-in-Q virtual switch:

```
dhcpv6 ldra set vs-port <port-object-list> vs <vs-object>
[vlan <vlan>] trust-mode {client-trusted |server-trusted
| dualrole-trusted | untrusted}
```

where

vs-port <port-object>
is the virtual switch port list.

vs <vs-object-list>
is the virtual switch.

vlan <vlan>
is the VLAN.

trust-mode {client-trusted | server-trusted | dualrole-trusted | untrusted}
is the trust mode. For descriptions, see the list of LDRA trust modes.

12 Set the values for the interface-ID and remote ID for the VLAN or virtual switch and port:

```
dhcpv6 ldra set vs-port-object-list> vs <vs-object>[VLAN
<VLAN>]{[intid-string <interfaceID-string>] [rid-string
<remoteID-string>]}
```

where

vs-port-object-list	is the virtual switch port list.
vs <vs-object-list>	is the virtual switch object list.
vlan <VLAN>	is the VLAN.
intid-string <interfaceID-string>	is the value used for the interface-ID option for this VLAN and port. Valid values are 1 to 64.
rid-string <remoteID-string>	is the value used for the remote-ID option for this VLAN and port. Note that the remote-id-option must be enabled for this value to be included. Valid values are 1 to 64.

13 Enable LDRA for the specified Q-in-Q virtual switch:

```
dhcpv6 ldra enable <vs-object>
```

14 Confirm the configuration:

```
dhcpv6 ldra show <vs-object-list>
```

where

vs-object-list	is the virtual switch that you want to view LDRA configuration for.

To configure LDRA on an MPLS virtual circuit

15 Enable LDRA:

```
dhcpv6 ldra enable
```

16 Create LDRA for the specified VLAN(s) or virtual switch(es):

```
dhcpv6 ldra create {<vlan-object-list>|<vs-object-list>}
```

17 Set LDRA attributes:

```
dhcpv6 ldra set {[interface-id-type {slot-port|slot-port-
vlan|intid-string}] [remote-id-type {device-mac|device-
hostname|rid-string}] [remote-id-enterprise-number
<enterprise-number>] [remote-id-option {on|off}]}
```

where

interface-id-type {slot-port| slot-port-vlan| intid-string}	is the value type for the interface-ID option of relay-forward messages. The default value is slot-port.
remote-id-type {device-mac| device-hostname|rid-string}	is the value type for the remote-id option of relay-forward messages. The default value is device-mac.
remote-id-enterprise-number <enterprise-number>	is the enterprise-number used in the remote-id option. Valid values are 1 to 4294967295. The default value is 3561, which is the Broadband Forum enterprise number. The Ciena enterprise number is 1271.
remote-id-option {on|off}	indicates whether to include the remote-id option in relay-forward messages. The default value is off.

18 Set the trust mode of LDRA on the VLAN and port:

```
dhcpv6 ldra set mpls-vc <vc-name> vs <vs-object> trust-
mode {client | server-trusted | dualrole-trusted |
untrusted}
```

where

mpls-vc <vc-name>	is the MPLS virtual circuit name.
vs <vs-object-list>	is the virtual switch.
trust-mode {client | server-trusted | dualrole-trusted | untrusted}	is the trust mode. MPLS-VC can only be server trusted or untrusted. For descriptions, For descriptions, see the list of LDRA trust modes.

19 If LDRA is configured to use intid-string and/or rid-string, set the values for interface-ID and remote ID for the VLAN or virtual switch and port:

```
dhcpv6 ldra set vs-port-object-list> vs <vs-object-
list>[<vlan>]{[intid-string <interfaceID-string>] [rid-
string <remoteID-string>]}
```

where

vs-port-object-list	is the virtual switch port list.
vlan <VLAN>	is the VLAN.
port <port list>	is the port list.
intid-string <interfaceID-string>	is the value used for the interface-ID option for this VLAN and port. Valid values are 1 to 64.
rid-string <remoteID-string>	is the value used for the remote-ID option for this VLAN and port. Note that the remote-id-option must be enabled for this value to be included. Valid values are 1 to 64.

20 Enable LDRA for the specified VLAN or VLANs:

```
dhcpv6 ldra enable {vlan <VLAN>|vs <vs>}
```

21 Confirm the configuration:

```
dhcpv6 ldra show [{<vlan-object-list>|<vs-object-list>}]
```

where

vlan-object-list>	is the VLAN that you want to view LDRA configuration for.
vs-object-list	is the virtual switch that you want to view LDRA configuration for.

—end—

Examples

This example configures an LDRA on a VLAN.

```
dhcpv6 ldra enable
dhcpv6 ldra create vlan 111
dhcpv6 ldra set circuit-id-type cid-string
dhcpv6 ldra set vlan 111 port 10 cid-string "Caller-ID
Text" trust-mode server-trusted
dhcpv6 ldra enable vlan 111
```

This example configures an LDRA on a QiQ virtual switch.

```
dhcpv6 ldra enable
dhcpv6 ldra create vs testQinQRelay
dhcpv6 ldra set interface-id-type intid-string
dhcpv6 ldra set vs-port 1,2 vs testQinQRelay vlan 100
trust-mode client-trusted
dhcpv6 ldra set vs-port 10 vs testQinQRelay trust-mode
server-trusted
dhcpv6 ldra set vs-port 1 vs testQinQRelay vlan 100 intid-
```

```
string PORT1
dhcpv6 ldra set vs-port 2 vs testQinQRelay vlan 100 intid-
string PORT2
dhcpv6 ldra enable vs testQinQRelay
```

This example configures an LDRA on a MPLS-VC.

```
dhcpv6 ldra enable
dhcpv6 ldra create vs testMPLSRelay
dhcpv6 ldra set vs-port 1,2 vs testMPLSRelay vlan 100
trust-mode client-trusted
dhcpv6 ldra set mpls-vc VCPrimary vs testMPLSRelay trust-
mode server-trusted
dhcpv6 ldra set mpls-vc VCSecondary vs testMPLSRelay
trust-mode server-trusted
dhvpv6 ldra enable vs testMPLSRelay
```

Procedure 3-14
Displaying and clearing relay agent statistics

You can display:

- L2 DHCP relay agent statistics
- LDRA statistics

You can clear:

- L2 DHCP relay agent global statistics
- LDRA global statistics
- L2 DHCP relay agent statistics
- LDRA statistics

Relay agents track these global statistics:

- total number of frames relayed by the relay agents
- total number of frames dropped by the relay agents
- total number of frame forwarded or passed to the relay agent but did not require processing
- not for relay frames passed to the relay that the relay did not expect. These frames are dropped.

L2 DHCP relay agents track these statistics for each VLAN or virtual switch:

- packets that contain IP security headers
- packets with option 82 added
- packets with option 82 removed
- packets where adding option 82 exceeds the MTU
- packets dropped due to being received on an untrusted client port
- packets dropped due to being received on an untrusted server port
- packets dropped due to spoofed DHCP packets
- packets dropped because there were no trusted server ports
- packets dropped because there were no trusted client ports
- packets dropped because of the relay configuration
- general errors

LDRAs track these statistics for each VLAN:

- packets for relay
- relayed client messages

- relayed server messages
- packets dropped due to being received on untrusted client port
- packets dropped due to being received on an untrusted server port
- packets dropped due to failed validation
- packets dropped because of the relay configuration
- packets dropped because the hop count was exceeded
- packets dropped because the relay frame exceeded the MTU
- packets dropped because there were no trusted server ports
- packets dropped because there were no trusted client ports
- packets dropped due to IPv6 fragmented or bad headers
- general errors

Step Action

To display L2 relay agent statistics

1 Display L2 relay agent statistics for a specified VLAN(s) or virtual switch:

```
dhcp l2-relay-agent show {<vlan-object-list>|<vs-object-list>} statistics
```

where

vlan-object-list	is the VLAN.
vs-object-list	is the virtual switch.

To display LDRA statistics

2 Display LDRA statistics for a specified VLAN(s) or virtual switch:

```
dhcpv6 ldra show {<vlan-object-list>|<vs-object-list>}
statistics
```

where

vlan-object-list	is the VLAN.
vs-object-list	is the virtual switch.

To clear L2 DHCP relay agent global statistics

3 Clear L2 DHCP relay agent global statistics:

```
dhcp l2-relay-agent clear statistics
```

To clear LDRA global statistics

4 Clear LDRA global statistics:

```
dhcpv6 ldra clear statistics
```

To clear L2 DHCP relay agent statistics

5 Clear L2 DHCP relay agent statistics:

```
dhcp l2-relay-agent clear {<vlan-object-list>|<vs-object-list>} statistics
```

where

vlan-object-list	is the VLAN.
vs-object-list	is the virtual switch.

To clear LDRA statistics

6 Clear LDRA statistics:

```
dhcpv6 ldra clear {<vlan-object-list>|<vs-object-list>}
statistics
```

where

vlan-object-list	is the VLAN.
vs-object-list	is the virtual switch.

—end—

Example

This example shows sample output for the dhcpv6 ldra show vlan <VLAN> statistics command, where the VLAN is MyVLAN.

```
dhcpv6 ldra show vlan MyVLAN statistics

+------------------ MyVLAN LDRA Statistics --------------------+
| Statistic                                      | Value       |
+------------------------------------------------+-------------+
| Packets for relay                              | 0           |
| Relayed Client messages                        | 0           |
| Relayed Server messages                        | 0           |
| Packets dropped: rx on untrusted client port   | 0           |
| Packets dropped: rx on untrusted server port   | 0           |
| Packets dropped: failed validation             | 0           |
| Packets dropped: relay configuration           | 0           |
| Packets dropped: exceeded hop count            | 0           |
| Packets dropped: relay frame exceeded MTU      | 0           |
| Packets dropped: no trusted server ports       | 0           |
| Packets dropped: no trusted client ports       | 0           |
| Packets dropped: IPv6 fragmented/bad header    | 0           |
| General Errors                                 | 0           |
+------------------------------------------------+-------------+
```

Procedure 3-15
Displaying LDRA information

Display LDRA information to view the global LDRA configuration and a summary of the VLANs or virtual switches.

Step **Action**

1 Display LDRA information:

```
dhcpv6 ldra show [{vlan-object-list>|vs-object-list>}]
```

where

vlan-object list is the VLAN (s) that you want to view LDRA configuration for.

vs-object-list is the virtual switch that you want to view the LDRA configuration for.

—end—

Example

This example shows sample output for the dhcpv6 ldra show command.

```
+--------- LDRA GLOBAL SETTINGS ---------+
| Setting            | Value             |
+--------------------+-------------------+
| Global Admin       | Disabled          |
| Interface ID Type  | Slot-Port         |
| Remote ID Option   | Off               |
| Remote ID Type     | MAC Addr          |
| RID Enterprise No. | 3561              |
+--------------------+-------------------+

+---------- LDRA GLOBAL STATISTICS ------+
| Statistic          | Value             |
+--------------------+-------------------+
| Relayed            | 0                 |
| Dropped            | 0                 |
| Forwarded          | 0                 |
| Not For Relay      | 0                 |
+--------------------+-------------------+

+--------------------- LDRA STATE ----------------------+
| VLAN ID |  VS Name        | Admin State | Oper State  |
+---------+-----------------+-------------+-------------+
| No LDRA entries found                                 |
+---------+-----------------+-------------+-------------+

+----------------------- TRUSTED PORT SETTINGS -----------------------+
| VLAN    |  Port        | SubVLAN | isActive     | Trust Mode        |
+---------+--------------+---------+--------------+-------------------+
| No port entries were found                                          |
+---------+--------------+---------+--------------+-------------------+
+-------------------------- INTID STRING SETTINGS ---------------------------+
| VLAN    | Port         | SubVLAN | Interface ID String                     |
+---------+--------------+---------+-----------------------------------------+
| No INTID String entries were found                                         |
+---------+--------------+---------+-----------------------------------------+

+--------------------------- RID STRING SETTINGS ----------------------------+
| VLAN    | Port         | SubVLAN | Remote ID String                        |
+---------+--------------+---------+-----------------------------------------+
| No RID String entries were found                                           |
+---------+--------------+---------+-----------------------------------------+
```

Procedure 3-16
Configuring the DNS client

The system supports up to three domain name servers that can be prioritized by the administrator. This functionality resolves host names to IP addresses. By default the DNS client is enabled, although no servers are configured.

DNS servers can be configured by means of DHCP or manually. When both DHCP and the user configure a set of DNS servers, the servers configured by DHCP are active, that is, operationally enabled, and the other servers are inactive.

The network element must have DNS servers defined if it is configured as a client resolver. A device does not do random DNS resolves if the DNS servers have not been configured.

These IP addresses cannot be specified as DNS servers:

- 0.0.0.0
- 224.0.0.0 -> 255.255.255.255
- 127.0.0.0 -> 127.255.255.255
- IPv6 addresses such as ff::/16 (multicast) or ::/0 (all zeros)

An error is returned if an IP address is not resolved.

Configuring the DNS client

- add a DNS server to the DNS list
- disable the DNS client
- disable the DNS server
- enable the DNS client
- enable the DNS server
- add a DNS server to the DNS list
- remove a DNS server
- resolve an IP address or hostname
- define the default domain name that is appended to unqualified host names
- set relative priority of a DNS server
- unset DNS client attributes

Step	Action

To add a DNS server to the DNS list

1 Add a DNS server to the DNS list:

```
dns-client add server <IP address>
```

where

server <IP address>	is the IP address of the DNS server.

To globally administratively disable the DNS client

2 Disable a DNS client:

```
dns-client disable
```

To disable a DNS server

3 Disable a DNS server:

```
dns-client disable server <IP address>
```

where

server <IP address>	is the IP address of the DNS server to disable.

To globally enable the DNS client

4 Enable a DNS client:

```
dns-client enable
```

To enable a DNS server

5 Enable a DNS server:

```
dns-client enable server <IP address>
```

where

server <IP address>	is the IP address of the DNS server to disable.

To add a DNS server to the DNS list

6 Add a DNS server to the DNS list:

```
dns-client add server <IP address>
```

where

server <IP address>	is the IP address of the DNS server.

To remove a DNS server

7 Remove a DNS server:

```
dns-client remove server <IP address>
```

where

server <IpAddress>	is the IP address of the DNS server.

To resolve an IP address or hostname

8 Resolve an IP address or hostname:

```
dns-client resolve ip <IP address or hostname>
```

where

ip <IP address or hostname>	is the host name or IP address to resolve.

To define the default domain name that is appended to unqualified host names

9 Define the default domain name that is appended to unqualified host names:

```
dns-client set domain-name <Domain-Name String[1..63]>
```

where

<Domain-Name String[1..63]>	is the DNS domain name

To set relative priority DNS server

10 Set relative priority DNS server:

```
dns-client set server <server> priority <NUMBER: 1..3>
```

where

server <server>	is the IP address of a configured DNS server.
priority <NUMBER: 1-3>	is the relative priority of DNS server.

To unset DNS client domain name attributes

11 Unset DNS client domain name attributes:

```
dns-client unset domain-name
```

—end—

Procedure 3-17
Displaying DNS client information

Display DNS client information.

Step **Action**

1 Display DNS client information:

```
dns-client show [domain-name] [servers] [monitor]
```

where the original parameters are	
domain-name	is DNS client domain name configuration information.
servers	is DNS client server configuration information.
monitor	is DNS client monitor information.

—end—

Procedure 3-18
Configuring global l3 DHCP relay agent instances

You can configure l3 DHCP relay instances globally or at the interface level, as demonstrated in "Configuring interface-level l3 DHCP relay agent instances" on page 3-70.

Administrative level access is required for these commands.

Step **Action**

To create a global l3 DHCP relay agent instance

Note: Only one l3 DHCP relay agent instance is allowed.

1 Create a global l3 DHCP relay agent instance:

```
dhcp l3-relay-agent instance <create | delete> dhcp-
instance <dhcp-instance-name>
```

where

<create | delete>	is the action for the global l3 DHCP relay instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

To enable a global l3 DHCP relay agent instance

2 Enable a global l3 DHCP relay agent instance:

```
dhcp l3-relay-agent instance <enable | disable> dhcp-
instance <dhcp-instance-name>
```

where

<enable | disable>	is the action for the global l3 DHCP relay instance. Default is enabled for the configured instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

To set a trust mode for the specific port used for a global l3 DHCP relay agent instance

3 Set a trust mode for the specific port used for a global l3 DHCP relay agent instance:

```
dhcp l3-relay-agent instance <set | unset> dhcp-instance
<dhcp-instance-name> trust-mode <trusted | untrusted>
```

where

<set | unset>	is the action for the global l3 DHCP relay instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.
<trusted | untrusted>	All attached ports are untrusted by default.

To configure the server address for the global l3 DHCP relay agent instance

Note: You can configure up to eight server addresses for a single global l3 DHCP relay agent instance.

4 Configure the server address for the global l3 DHCP relay agent instance:

```
dhcp l3-relay-agent instance <add | remove> dhcp-instance
<dhcp-instance-name> server-addr <server-ip>
```

where

<add | remove>	is the action for the global l3 DHCP relay instance server address.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.
<server-ip>	is the IP address of the server used for this global l3 DHCP relay instance.

To enable option 82 for relay requests

5 Enable option 82 for relay requests for the global l3 DHCP relay instance:

```
dhcp l3-relay-agent instance <set | unset> dhcp-instance
<dhcp-instance-name> option82 <on | off | replace>
```

where

<set | unset>	is the action for the global l3 DHCP relay instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.
<on | off | replace>	is where option 82 is enabled for relay requests. Default is off.

To set the remote ID type

6 Set the remote ID type for the global l3 DHCP relay instance:

```
dhcp l3-relay-agent instance <set | unset> dhcp-instance
<dhcp-instance-name> remote-id-type <device-hostname |
device-mac | rid-string>
```

where

<set | unset>	is the action for the global l3 DHCP relay instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.
<device-hostname | device-mac | rid-string>	is the remote ID type value. Default is device-mac.

To set the circuit ID type

7 Set the circuit ID type for the global l3 DHCP relay instance:

```
dhcp l3-relay-agent instance <set | unset> dhcp-instance
<dhcp-instance-name> circuit-id-type <cid-string |
interface-name>
```

where

<set | unset>	is the action for the global l3 DHCP relay instance.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.
<cid-string | interface-name>	is the circuit ID type value. Default is interface-name.

To display global l3 DHCP relay instance information

8 Display global l3 DHCP relay instance-specific configuration:

```
dhcp l3-relay-agent instance show dhcp-instance <dhcp-
instance-name>
```

where

<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

9 Display global l3 DHCP relay instance statistics:

```
dhcp l3-relay-agent instance show dhcp-instance <dhcp-
instance-name> statistics
```

where

<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

To clear global l3 DHCP relay instance statistics

10 Clear global l3 DHCP relay instance statistics:

```
dhcp l3-relay-agent instance clear dhcp-instance <dhcp-
instance-name> statistics
```

where

<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

To set the global l3 DHCP relay instance debug logging level

11 Set the global l3 DHCP relay instance debug logging level:

```
dhcp l3-relay-agent debug <info | error | debug |show>
```

where

<info | error | debug | show>	is the debug logging level for the global l3 DHCP relay instance.

—end—

Examples

Here are output samples of the “show” command for global l3 DHCP relay instances:

```
> dhcp l3-relay-agent instance show dhcp-instance dhcp1

+-------------L3 RELAY INSTANCE TABLE--------------------+
| Parameter            | Value                           |
+----------------------+---------------------------------+
| Instance Name        | dhcp1                           |
| Admin State          | Disabled                        |
| Oper  State          | Disabled                        |
| Circuit ID Type      | CID-String                      |
| Remote ID Type       | RID-String                      |
| Option82             | Off                             |
| Trust mode           | Trusted                         |
| Server Addresses     | 3.3.3.2                         |
|                      | 3.3.3.4                         |
+----------------------+---------------------------------+


> dhcp l3-relay-agent instance show dhcp-instance dhcp1 statistics

+--------------------L3 RELAY GLOBAL STATISTICS----------------------+
| Statistic                                   | Value                |
+---------------------------------------------+----------------------+
| Total Packets Relayed                       | 0                    |
| Total Packets Dropped                       | 0                    |
| Total Requests Received                     | 0                    |
| Total Response Received                     | 0                    |
| Option 82 Replaced                          | 0                    |
| Option 82 Added                             | 0                    |
| Option 82 Untouched                         | 0                    |
| Bad Circuit ID                              | 0                    |
| Client spoofed packets                      | 0                    |
| Server spoofed packets                      | 0                    |
+---------------------------------------------+----------------------+

+-------------------L3 RELAY STATISTICS PER SERVER-------------------+
| Statistic Server (3.3.3.2)                  | Value                |
+---------------------------------------------+----------------------+
| Total Requests Relayed                      | 0                    |
| Error during Relay                          | 0                    |
+---------------------------------------------+----------------------+

+-------------------L3 RELAY STATISTICS PER SERVER-------------------+
| Statistic Server (3.3.3.4)                  | Value                |
+---------------------------------------------+----------------------+
| Total Requests Relayed                      | 0                    |
| Error during Relay                          | 0                    |
+---------------------------------------------+----------------------+
```

Procedure 3-19
Configuring interface-level l3 DHCP relay agent instances

You can configure l3 DHCP relay agent instances at the interface level or globally, as demonstrated in “Configuring global l3 DHCP relay agent instances” on page 3-66.

Administrative level access is required for these commands.

Step Action

To attach an IP interface to the l3 DHCP relay instance

1 Attach an IP interface to the l3 DHCP relay instance:

```
dhcp l3-relay-agent interface <attach | detach> ip-interface <interface-name> dhcp-instance <dhcp-instance-name>
```

where

<attach | detach>	is the action for the l3 DHCP relay interface.
<interface-name>	is the name of the l3 DHCP relay interface.
<dhcp-instance-name>	is the name of the global l3 DHCP relay instance.

To enable the attached IP interface

2 Enable the attached IP interface:

```
dhcp l3-relay-agent interface <enable | disable> ip-interface <interface-name>
```

where

<enable | disable>	is the action for the l3 DHCP relay interface. Attached interfaces are enabled by default.
<interface-name>	is the name of the l3 DHCP relay interface.

To configure the circuit ID string for a specific IP interface

3 Configure the circuit ID string:

```
dhcp l3-relay-agent interface <set | unset> ip-interface <interface-name> cid-string <cid-string>
```

where

<set | unset>	is the action for the l3 DHCP relay interface.
<interface-name>	is the name of the l3 DHCP relay interface.
<cid-string>	The interface name is used as the cid-string by default.

To configure the remote ID string for a specific IP interface

4 Configure the remote ID string:

```
dhcp l3-relay-agent interface <set | unset> ip-interface
<interface-name> rid-string <rid-string>
```

where

<set | unset>	is the action for the l3 DHCP relay interface.
<interface-name>	is the name of the l3 DHCP relay interface.
<rid-string>	The system MAC address is used as the rid-string by default.

To configure the trust mode on an IP interface

5 Configure the trust mode on an IP interface:

```
dhcp l3-relay-agent interface <set | unset> ip-interface
<interface-name> trust-mode <trusted | untrusted>
```

where

<set | unset>	is the action for the l3 DHCP relay interface.
<interface-name>	is the name of the l3 DHCP relay interface.
<trusted | untrusted>	All attached ports are untrusted by default.

To configure the trust mode on the port or VLAN of an IP interface

6 Configure the trust mode on the port or VLAN of an IP interface:

```
dhcp l3-relay-agent interface <set | unset> ip-interface
<interface-name> port <port-num> trust-mode <trusted |
untrusted>
```

where

<set | unset>	is the action for the l3 DHCP relay interface.
<interface-name>	is the name of the l3 DHCP relay interface.
<trusted | untrusted>	All attached ports are untrusted by default.

To display l3 DHCP relay interface information

7 Display all information for the interface to the l3 DHCP relay instance:

```
dhcp l3-relay-agent interface show
```

8 Display detailed information for the specific interface to the l3 DHCP relay instance:

```
dhcp l3-relay-agent interface show ip-interface
<interface-name>
```

where

<interface-name>	is the name of the l3 DHCP relay interface.

9 Display l3 DHCP relay interface statistics:

```
dhcp l3-relay-agent interface show ip-interface
<interface-name> statistics
```

where

<interface-name>	is the name of the l3 DHCP relay interface.

To clear l3 DHCP relay interface statistics

10 Clear l3 DHCP relay interface statistics:

```
dhcp l3-relay-agent instance clear interface <interface-
name> statistics
```

where

<interface-name>	is the name of the l3 DHCP relay interface.

To set the l3 DHCP relay interface debug logging level

11 Set the l3 DHCP relay interface debug logging level:

```
dhcp l3-relay-agent debug <info | error | debug |show>
```

where

<info | error | debug | show>	is the debug logging level for the l3 DHCP relay interface

—end—

Examples

Here are output samples of the “show” command for l3 DHCP relay interfaces:

```
> dhcp l3-relay-agent interface show

+-------------------------L3 RELAY INTERFACE STATE--------------------+
| Interface name  | Trust Mode | Relay Admin State | Relay Oper State |
+-----------------+------------+-------------------+------------------+
| xyz             | Untrusted  | Enabled           | Enabled          |
| vlan12345678912 | Ignore     | Enabled           | Enabled          |
| abc1            | Trusted    | Enabled           | Enabled          |
+-----------------+------------+-------------------+------------------+


> dhcp l3-relay-agent interface show ip-interface vlan12345678912

+----------------L3 RELAY INTERFACE SETTINGS------------------------------+
| Parameter         | Value                                               |
+-------------------+-----------------------------------------------------+
| Name              | vlan12345678912                                     |
| Type              | Vlan                                                |
| Relay Admin State | Enabled                                             |
| Relay Oper State  | Enabled                                             |
| Trust mode        | Ignore                                              |
| Circuit-ID        | v12345678912345678912345678912345678912345678912345 |
|                   | (Max length 255 truncated to 5 lines)               |
|                   | 6789123456789123456789123456789123456789123456789v1 |
|                   | 234567891234567891234567891234567891234567891234567 |
|                   | 891234567891234567891234567891234567891234567898912 |
|                   | 345678912345678912345678912345678912345678912345678 |
| Remote-ID         | v123456789123456789123456789123456789123456789123451 |
|                   | 67891234567891234567                                |
+-------------------+-----------------------------------------------------+


+-----------PORT TRUST MODE SETTINGS---------+
| Interface name  | Vlan | Port | Trust Mode |
+-----------------+------+------+------------+
| vlan12345678912 | 33   | 4    | Ignore     |
|                 | 33   | 8    | Untrusted  |
+-----------------+------+------+------------+


> dhcp l3-relay-agent interface show ip-interface serverInterface statistics

+---------------------RELAY INTERFACE STATISTICS---------------------+
| Statistic                                   | Value                |
+---------------------------------------------+----------------------+
| Requests on untrusted interface             | 0                    |
| Response on untrusted interface             | 0                    |
| Response Forwarded                          | 0                    |
| Response Packet Error                       | 0                    |
| L3 Agent option Error                       | 0                    |
+---------------------------------------------+----------------------+
```

Procedure 3-20
Configuring NTP

Configuring NTP includes these tasks:

- setting the mode for NTP client
- globally enable NTP client
- globally disable NTP client
- enabling notifications
- disabling notifications

Step Action

To set the mode for NTP

1 Determine the mode that you want to set.

If you want to set the mode to	Then
broadcast	Perform step 2.
multicast	Perform step 3.
polling and specify a polling interval	Perform step 4.

2 Set the mode to broadcast:

```
ntp client set mode broadcast
```

Note 1: When the device is set in broadcast mode, setting a polling-interval is ignored by the device.

Note 2: In broadcast mode, you do not need to configure the NTP client to use a specific server. Instead, the NTP client waits for broadcast servers on the same subnet to broadcast their current time. When the NTP client receives the first message, the client interacts with that server to retrieve reliable time. When additional broadcast messages are received from that server, the NTP client calculates the time difference and adjust the clock accordingly. If broadcast messages are received from several broadcast servers, the client selects the most accurate server to use.

3 Set the mode to multicast:

```
ntp client set mode multicast
```

Note: NTP servers synchronize with IPv4 broadcast servers when NTP client mode is set to multicast for IPv6. In multicast mode, SAOS can synchronize with IPv6 and IPv4 using broadcast traffic. NTP client synchronizes with the possible time available, IPv4 or IPv6.

4 Set the mode to polling and specify a polling interval:

```
ntp client set mode polling polling-interval <SECONDS:
16,32,64,128,256,512,1024,2048,4096>
```

Note: Any number can be entered for the interval value, but the system rounds the number down to the nearest allowed value, as shown in the example.

5 Set the minimum and maximum polling intervals:

```
ntp client set mode min-polling-interval <SECONDS:
16..4096> max-polling-interval <SECONDS: 16..4096>
```

To enable the NTP client

6 Enable the NTP client:

```
ntp client enable
```

To disable the NTP client

7 Disable the NTP client:

```
ntp client disable
```

To enable notifications

8 Enable notifications:

```
ntp client set sync-change-notification on
```

To disable notifications

9 Disable notifications:

```
ntp client set sync-change-notification off
```

Example

This example selects the polling mode and sets the polling interval to 1000.

```
> ntp client set polling-interval 1000

Polling time has been adjusted to 512 seconds
```

Procedure 3-21
Configuring NTP servers

You can add a list of NTP servers directly or with a DHCP server using option 42 as shown in “Configuring DHCP client”.

If desired, you can enable notifications so that when time is synchronized with the NTP server, the system generates event and Syslog messages with NTP time and system uptime. By default, these notifications are disabled.

Step Action

To add an NTP server for broadcast or polling modes

1 Add an NTP server to the client to be used for broadcast or polling modes:

```
ntp client add server <IP address or host name[1..63]
[key-id <NUMBER: 1..65534>]
```

where

server <IP address or host name[1..63]	is the host name or IP address of the NTP server to be added.
[key-id <NUMBER: 1..65534>]	is the authentication key identifier to be used for the NTP server. The default is NO key.

To add an NTP multicast server for multicast mode

2 Add an NTP multicast server to the client to be used for multicast mode:

```
ntp client add multicast-server <IPv6 address[1..63]>
```

where

<IP address[1..63]>	is the IPv6 address of the multicast server to be added.

To remove an NTP server

3 Remove an NTP server:

```
ntp client remove server <server>
```

where

server <server>	is the host name or IP address of the configured NTP server to be removed.

To remove a multicast server

4 Remove a multicast server:

```
ntp client remove multicast-server <multicast-server>
```

where

<multicast-server> is the IPv6 address of the configured multicast server to be removed.

To enable an NTP client server

5 Enable the NTP client server:

```
ntp client enable <server>
```

where

<server> is the host name or IP address of the configured NTP server being enabled.

To disable the NTP client server

6 Disable the NTP client server:

```
ntp client disable <server>
```

where

<server> is the host name or IP address of the configured NTP server being disabled.

—end—

Procedure 3-22
Adding NTP servers to the NTP client server list

Add NTP servers to the NTP client server list.

Step	Action
1	Add a minimum of three NTP servers to the NTP client server list: `ntp client add server 192.2.3.4`

—end—

Examples

This example adds NTP servers to the NTP client server list.

```
ntp client add server 192.2.3.4
ntp client add server 192.6.7.8
ntp client add server 192.9.10.11
ntp client add server wadc01.ciena.com
ntp client add server 10.10.121.73 key 4
```

This example shows the output from the ntp client show command for the above configuration:

```
> ntp client show

+------------------- NTP CLIENT STATE -------------------+
| Parameter                | Value                       |
+--------------------------+-----------------------------+
| Admin State              | Enabled                     |
| Auth Admin State         | Disabled                    |
| Mode                     | Polling                     |
| Polling Interval (min)   | 16                          |
| Polling Interval (max)   | 16                          |
| Config State             | user                        |
| DHCP NTP Option State    | On                          |
| Sync Notification        | Off                         |
| Delay  (ms)              | 0.000                       |
| Offset (ms)              | 0.000                       |
| Jitter (ms)              | 0.000                       |
| Drift  (ppm)             | 0.000                       |
| Synchronized             | False                       |
+--------------------------+-----------------------------+

+-----------------------------------NTP SERVER CONFIGURATION-----------------------------------------+
| IP          |Host               | Auth    | Config | Admin | Oper  | Server | Server    | Auth  | Offset |
| Address     |Name               | Key ID  | State  | State | State | State  | Condition | state | (ms)   |
+-------------+-------------------+---------+--------+-------+-------+--------+-----------+-------+--------+
| 10.10.121.73 | 10.10.121.73     | 4       | user   | Ena   | Ena   | Reach  | sys Peer  | None  |        |
| 192.2.3.4    | 192.2.3.4        | 0       | user   | Ena   | Ena   | UnReac | Reject    | None  | 0.000  |
| 10.10.21.22  | wadc01.ciena.com | 0       | user   | Ena   | Ena   | Reach  | Sys Peer  | None  |        |
+--------------+------------------+---------+--------+-------+-------+--------+-----------+-------+--------+
+- NTP AUTHENTICATION KEYS -+
| Key ID      | Type        |
+-------------+-------------+
| 4           | md5         |
+-------------+-------------+

+-------------------------- NTP MULTICAST ADDRESSES ---------------------------+
| NO ENTRIES                                                                    |
+------------------------------------------------------------------------------+
```

Procedure 3-23
Configuring NTP authentication

NTP supports MD5 authentication and SHA-1 authentication. Configuring NTP authentication consists of these tasks:

- enabling authentication
- disabling authentication
- adding keys
- importing keys
- removing keys
- displaying configuration information

By default, MD5 authentication is disabled for the NTP client.

You can add up to 40 authentication keys, as shown in this table.

Table 3-10
Authentication keys

Authentication Key	**Valid Values**
Key ID	U40 value between 1 and 4294967295. If a key ID is entered or displayed as 0, this value implies there is no key.
SHA-1 key	40-character hexadecimal digit string
MD5 key	1 to 40 ASCII character string that cannot be any of the following: • space () • double quote (“) • number sign (#) • tab (\t) • return (\n) • \0

There are two ways to add a key:

- enter plain text directly
- transfer a simple tag-readable format file to the system and then import keys from it

When importing keys from a tag-readable format file, the importing key file is in this format:

```
<key-id> <type> <encrypted-key-value>
```

This example shows a key file that is ready to import:

```
1 MD5 !ZS,@S~(\D&1k0V'   # MD5 key
2 MD5 yz3O$2*>oS(>o2Mf   # MD5 key
3 MD5 T/oI/Hqa!,|NQYgq   # MD5 key
4 SHA1 098ff18eea4abff26e81722c72faf7c345033119 # SHA1
key
5 SHA1 da0261d0451785086ff327751713aa225a871f25 # SHA1
key
6 SHA1 61d624c9420c07fb70d1078a065e706c031746ed #S HA1
key
```

Keys imported from a file are subsequently saved in the configuration file when the configuration save command is executed.

Step	Action

To enable NTP server authentication

1 Enable authentication on the NTP server:

```
ntp authentication enable
```

To disable NTP server authentication

2 Disable authentication on the NTP server:

```
ntp authentication disable
```

To add an MD5 key

3 Add an MD5 key:

```
ntp authentication add key-id <NUMBER: 1..65534> md5 <MD5
auth key [1..40]>
```

where

key-id <NUMBER>	is the NTP MD5 key object.
md5 <MD5 auth key [1..40]>	is the MD5 authentication key.

To add an SHA1 key

4 Add an SHA-1 key:

```
ntp authentication add key-id <NUMBER: 1..65534> sha1
<SHA-1 auth key [1..40]>
```

where

key-id <NUMBER>	is the NTP SHA-1 key object.
sha1 <SHA-1 auth key>	is the SHA-1 authentication key.

To import a key from the NTP server

5 Import an authentication key from the NTP server:

```
ntp authentication import {filename <String>}
{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

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use 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.

where

password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535>	is the server-port number to connect to.

To remove a key from the NTP server

6 Remove an authentication key from the NTP server:

```
ntp authentication remove key-id <NUMBER: 1..65534>
```

where

key-id <NUMBER: 1..65534>	is the key identifier (SHA-1 or MD5). It is not necessary to specify the key type.

To display a key

7 Display MD5 configuration:

```
ntp authentication show
```

—end—

Examples

This example adds an MD5 key with an identifier of Key1.

```
ntp authentication add key-id 1 md5 Key1
```

This example adds an SHA-1 key with an identifier of Key40.

```
ntp authentication add key-id 20 sha1 Key40
```

This example removes a key that has a key-id of 1.

```
ntp authentication remove key-id 1
```

This example shows sample output for the ntp authentication show command.

```
> ntp authentication show

+------------------- NTP CLIENT STATE -------------------+
| Parameter               | Value                        |
+-------------------------+------------------------------+
| Admin State             | Enabled                      |
| Auth Admin State        | Enabled                      |
| Mode                    | Polling                      |
| Polling Interval (min)  | 16                           |
| Polling Interval (max)  | 16                           |
| Config State            | user                         |
| DHCP NTP Option State   | On                           |
| Sync Notification       | Off                          |
| Delay  (ms)             | 0.342                        |
| Offset (ms)             | 0.207                        |
| Jitter (ms)             | 0.078                        |
| Drift  (ppm)            | 0.000                        |
| Synchronized            | True                         |
+-------------------------+------------------------------+

+- NTP AUTHENTICATION KEYS -+
| Key ID      | Type        |
+-------------+-------------+
| 3           | sha1        |
| 7           | md5         |
+-------------+-------------+

+-----------------------------------NTP SERVER CONFIGURATION----------------------------------------------+
| IP                   |Host   | Auth      | Config | Admin | Oper  | Server | Server    | Auth  | Offset |
| Address              |Name   | Key ID    | State  | State | State | State  | Condition | state | (ms)   |
+----------------------+-------+-----------+--------+-------+-------+--------+-----------+-------+--------+
| 203.0.113.0          | tick  | 3         | user   | Ena   | Ena   | Reach  | sys Peer  | None  | 0.207  |
| 2001:db8::7310:0137  | tock  | 7         | user   | Ena   | Ena   | Reach  | Sys Peer  | None  | 0.275  |
+----------------------+-------+-----------+--------+-------+-------+--------+-----------+-------+--------+
```

Procedure 3-24
Clearing the drift file

Clear the NTP drift file when a system event causes the drift information to be inaccurate. Events that cause the drift information to become inaccurate include the:

- device time does not synchronize correctly with the NTP server
- drift value exceeds a specified value

Step	Action
1	Clear the NTP drift file: `ntp client clear drift`

—end—

Procedure 3-25
Displaying NTP state and configured servers

As the NTP client communicates with the server, the server state is updated. This table shows the status values you see when displaying NTP configuration while the NTP client communicates with NTP servers.

Table 3-11
Server Status

State Displayed	Description
Reject	Rejected or initial state.
Insane	Failed sanity check. Client has yet to be synchronized with the server.
Correct	Passed correctness check. Culled from the end of the candidate list.
Standby	Discarded by the clustering algorithm.
Candidate	Included in the final selection test.
Selected	Selected for synchronization; but distance exceeds maximum.
SysPeer	Selected for synchronization
PPSPeer	Selected for synchronization, PPS signal in use.
Reaching	Communicating with a potential candidate.
ERROR*	Error occurred with communication.

Note: The NTP state "Synchronized" parameter has a value of "false" until the NTP client has elected a system peer as shown by the server state of "SysPeer."

Step **Action**

To display NTP state and configured servers

1 Display NTP state and configured servers:

```
ntp client show
```

To display operational servers

2 Display operational servers:

```
ntp client show oper
```

To display NTP state only

3 Display NTP state only:

```
ntp client show state
```

To display NTP keys only

4 Display NTP state only:

```
ntp client show keys
```

To display a specific server configuration

5 Display a specific server configuration:

```
ntp client show server <server>
```

where

server <server>	is the IP address or hostname of the configured server that you want to display information for.

—end—

Example

This example shows sample output for the ntp client show command.

```
> ntp client show

+------------------- NTP CLIENT STATE -------------------+
| Parameter                | Value                       |
+--------------------------+-----------------------------+
| Admin State              | Enabled                     |
| Auth Admin State         | Disabled                    |
| Mode                     | Polling                     |
| Polling Interval (min)   | 16                          |
| Polling Interval (max)   | 16                          |
| Config State             | user                        |
| DHCP NTP Option State    | On                          |
| Sync Notification        | Off                         |
| Delay  (ms)              | 0.000                       |
| Offset (ms)              | 0.000                       |
| Jitter (ms)              | 0.000                       |
| Drift  (ppm)             | 0.000                       |
| Synchronized             | False                       |
+--------------------------+-----------------------------+

+-------------------------------------NTP SERVER CONFIGURATION----------------------------------------+
| IP           |Host              | Auth     | Config | Admin | Oper  | Server | Server    | Auth  | Offset |
| Address      |Name              | Key ID   | State  | State | State | State  | Condition | state | (ms)   |
+--------------+------------------+----------+--------+-------+-------+--------+-----------+-------+--------+
| 10.10.121.73 | 10.10.121.73     | 4        | user   | Ena   | Ena   | Reach  | sys Peer  | None  |        |
| 192.2.3.4    | 192.2.3.4        | 0        | user   | Ena   | Ena   | UnReac | Reject    | None  | 0.000  |
| 10.10.21.22  | wadc01.ciena.com | 0        | user   | Ena   | Ena   | Reach  | Sys Peer  | None  |        |
+--------------+------------------+----------+--------+-------+-------+--------+-----------+-------+--------+

+- NTP AUTHENTICATION KEYS -+
| Key ID      | Type        |
+-------------+-------------+
| 4           | md5         |
+-------------+-------------+
```

This example shows sample output for operational servers.

```
> ntp client show oper

+-------------------------------------- OPER NTP SERVERS ---------------------------------------+
| IP Address / Host Name                  |Server State|Server Condition|Auth Status| Offset(ms)|
+-----------------------------------------+------------+----------------+-----------+-----------+
|10.10.121.73                             |Reachable   |SysPeer         |None       |      0.098|
|192.2.3.4                                |Un-Reachable|Reject          |None       |      0.000|
|10.10.21.22                              |Reachable   |SysPeer         |None       |      0.101|
+-----------------------------------------+------------+----------------+-----------+-----------+


+-------------------------- NTP MULTICAST ADDRESSES ----------------------------+
| NO ENTRIES                                                                    |
+-------------------------------------------------------------------------------+
```

This example shows sample output for NTP state.

```
> ntp client show state
+------------------ NTP CLIENT STATE -------------------+
| Parameter              | Value                        |
+------------------------+------------------------------+
| Admin State            | Enabled                      |
| Auth Admin State       | Disabled                     |
| Mode                   | Polling                      |
| Polling Interval (min) | 16                           |
| Polling Interval (max) | 16                           |
| Config State           | user                         |
| DHCP NTP Option State  | On                           |
| Sync Notification      | Off                          |
| Delay  (ms)            | 89.288                       |
| Offset (ms)            | -0.138                       |
| Jitter (ms)            | 0.222                        |
| Drift  (ppm)           | 7.329                        |
| Synchronized           | True                         |
+------------------------+------------------------------+
```

This example shows sample output for a specific server configuration.

```
> ntp client show server 192.0.2.1
+-------------------------- NTP SERVER CONFIGURATION ---------------------------+
| Parameter   | Value                                                           |
+-------------+-----------------------------------------------------------------+
| Host Name   |                                                                 |
| IP Address  | 192.0.2.1                                                       |
| Admin State | Enabled                                                         |
| Oper State  | Enabled                                                         |
| Auth Key ID | 0                                                               |
| Config State| user                                                            |
| Server State| Un-Reachable                                                    |
|  Condition  | Reject                                                          |
|  Auth State | None                                                            |
|  Offset (ms)| 0.000                                                           |
+-------------+-----------------------------------------------------------------+
```

Procedure 3-26
Removing entries from the neighbor cache table

Remove entries from the neighbor cache table when the entries are no longer required.

Step **Action**

To flush a management interface ndp entry from the neighbor cache table

1 Flush the specified management interface entries from the neighbor cache table:

```
ndp flush interface <local | remote>
```

where

<local | remote>	is the interface to be flushed.

To flush an IP interface ndp entry from the neighbor cache table

2 Flush the specified management interface entries from the neighbor cache table:

```
ndp flush ip-interface <ip-interface>
```

where

<ip-interface>	is the IP address of the configured IP interface.

To remove an IP interface from the neighbor cache table

3 Removes the specified IP address from the neighbor cache table.

```
ndp delete ip-interface <ip-interface>
```

where

<ip-object>	is the IP address that you want to remove.
<intf-attr>	is the interface that you want to remove the ip address from.

To display the neighbors cache

4 Display the neighbors cache:

```
ndp show ip-interface <ip-interface>]
```

where.0

<ip-interface>	is the IP address of the configured IP interface.

—end—

System shell operations

This section provides the procedures needed to customize the switch after installation:

Procedure 4-1
Configuring the host name

The default host name is the model number of the device, such as 3942. The host name is displayed in the command prompt. You can set a custom host name to identify the device. The host name length is 2-63 characters without any spaces. At least one character must be alpha (a-z) or a dash (-). IP addresses are not allowed. The host name is not case sensitive. These special characters are not allowed:

“
%
*
?
!

To set the host name to the default, use the system unset host-name command.

Step	Action

To set the host name

1 Set the host name:

```
system set host-name <String[1..63]>
```

where

host-name <String[1..63]>	is the host name that you want to set for the device

To reset the host name

2 Reset the host name to default:

```
system unset host-name
```

—end—

Example

This example sets the host name to myHostName.

```
system set host-name myHostName
```

Procedure 4-2
Setting the date and time

Manually set the date and time as required. If NTP is enabled, all manual time and date settings are overridden by the NTP settings.

> ***Note:*** DHCPv4 client can set the time-offset, and DHCPv6 can set this by means of a named zone from the system-standard time zone database.

Step Action

To set the date and time

1 Set the date and time:

```
system set [date <yyyy-mm-dd>|<yy-mm-dd>|<mm-dd>] [time
<hh:mm:ss>|<hh:mm>] [time-offset <SECONDS: -
43200..50400>][timestamp <local|UTC>
```

where

date <yyyy-mm-dd>|<yy-mm-dd>|<mm-dd>	is the system date. Accepted formats are yyyy-mm-dd, yy-mm-dd, or mm-dd. If the yy-mm-dd format is used, the two digits are added to a base of 2000. For example, 03-01-07 becomes 2007-01-01. If you enter a date prior to 01-01-2004, the system automatically sets the date to 01-01-2004 on startup.
time <hh:mm:ss>|<hh:mm>	is the system time. Accepted formats are hh:mm:ss or hh:mm.
time-offset <SECONDS: -43200..50400>	is the time-offset in seconds from UTC. Value range is -43200..50400> seconds from UTC. Positive numbers are east of the UTC; negative numbers are west of the UTC.
timestamp <local|UTC>	is the timestamp for system logging entries. When set to 'local,' any system timestamps use the configured time-offset. When set to 'UTC,' system timestamps are based on UTC.

To unset the time offset and log timestamp

2 Unset the time offset and timestamp:

```
system unset [time-offset] [timestamp]
```

where

time-offset to default 0	resets the time off-set from UTC back.
timestamp back to default (local)	reset the timestamps for system logging entries.

To display the system date and time

3 Display the system date and time:

```
system show [date] {time} [time-offset]
```

—end—

Examples

This example sets the system date to June 18, 2007 and the system time to 09:33.

```
system set date 2007-06-18 time 09:33
```

This example sets the system time to 09:33 Pacific Daylight Time (PDT).

```
system set time 09:33 time-offset -25200
```

This example sets the system time to 09:33 Pacific Standard Time (PST).

```
system set time 09:33 time-offset -28800
```

This example sets the system time to 09:33 Eastern Daylight Time (EDT) USA.

```
system set time 09:33 time-offset -14400
```

This example sets the system time to 09:33 Eastern Standard Time (EST) USA.

```
system set time 09:33 time-offset -18000
```

Procedure 4-3
Configuring the inactivity timer

To free up inactive Telnet or SSH connections, you can configure the device to automatically end inactive connections by setting a global inactivity time-out and timer. By default, the time-out is 10 minutes, and the timer is turned on.

Step **Action**

To set the inactivity time-out to automatically end inactive connections after a period of inactivity and turn the inactivity timer on

1 Set the inactivity time-out to automatically end inactive connections after a period of inactivity and turn the inactivity timer on:

```
system shell set global-inactivity-timeout <MINUTES: 1-
1500> global-inactivity-timer on
```

where

<MINUTES: 1-1500>	is the length (in minutes) of inactivity before the user is logged out

To reset the global inactivity time-out and timer to default values

2 Reset the global inactivity time-out and timer to default values:

```
system shell unset global-inactivity-timeout global-
inactivity-timer
```

—end—

Procedure 4-4
Configuring lines to display

When a command result in the display of output exceeds the number of lines available on the session screen, the CLI emulates the Linux `more` command and pauses output until a user enters one of the following:

<CR>	Advance one line
<space>	Advance one page
q	Quit and do not display the remaining output
r	Display the rest of the output without pausing
t	tail, displays the last part (or tail end) of the output

You can configure settings for "more" and "more-lines" for your current session or globally for all sessions.

When you change a global setting, that change is immediately applied to your current session. Changing a global setting does not affect other users' existing sessions; it is applied to other users' new sessions only.

By default, “more” is enabled.

Step Action

To configure more lines for all sessions

1 Configure global more lines for all sessions:

```
system shell set global-more on global-more-lines
<NUMBER: 0-999>
```

where

global-more-lines <NUMBER: 0-999>	is the number of lines to display before presenting the options to display more lines for the current session. The default value is 0: the system determines the window size automatically.

To reset more lines for all sessions to the defaults

2 Reset more lines for all sessions to the defaults:

```
system shell unset global-more global-more-lines
```

To configure more lines for your current session

3 Configure more lines for your current session:

```
system shell session set more on more-lines <NUMBER: 0-
999>
```

where

<NUMBER: 0-999> is the number of lines to display before presenting the options to display more lines for the current session.

To reset more lines for your current session to the defaults

4 Reset more lines for your current session to the defaults:

```
system shell session unset more more-lines
```

—end—

Example

This example shows sample output when the more parameter is set to on and the more-lines parameter is set to 5.

```
> system shell session set more on more-lines 5
> system ?
health                        health management
set                           set system attributes
shell                         shell configuration
show                          show system attributes
--More--
```

Procedure 4-5
Configuring current session parameters

You can set the current session parameters.

Step Action

To configure more lines for your current session

1 Configure more lines for your current session:

```
system shell session set more on more-lines <NUMBER: 0-
999> tab-more on window-height <NUMBER: 0..999> window-
width <NUMBER: 0..999>
```

where

more-lines <NUMBER: 0..999> is the number of lines to display before presenting the options to display more lines for the current session.

window-height <NUMBER: 0..999> sets the session's window height.

window-width <NUMBER: 0..999> sets the session's window width.

To reset more lines for your current session to the defaults

2 Reset more lines for your current session to the defaults:

```
system shell session unset more more-lines
```

—end—

Example

This example shows sample output when the more parameter is set to on and the more-lines parameter is set to 5.

```
> system shell session set more on more-lines 5
> system ?
debug                         debug
guardian                      guardian settingss
server                        server control
ps                            information about system processes
[more 28%] (q,g,space,enter)
```

Procedure 4-6
Creating a banner file

You can create customized logon and welcome banner text files, and set your devices to display the file text when Telnet or SSH client sessions are established. You can create one file to display at the logon prompt and one to display after logging on or use the same file to display at both. You can configure the welcome banner using the device’s XML file or manually from the CLI.

> ***Note:*** Ensure that each line ends with an ASCII newline character. If a line does not end with an ASCII newline character, it does not display.

Step **Action**

1 Create a text file with the banner text.

2 Transfer the file to the device.

```
system xftp getfile {filename <String>}
{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

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use the default SFTP server.
tftp-server <ip-host-str>	is the tftp-server.
server-port <INTEGER: 1...65535>	is the server-port number.

where

ftp-server <ip-host-str>	is the sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

3 Verify that the file is stored.

—end—

Example

This example places the file myBannerFile.txt on the /flash0 directory of the device.

```
system xftp getfile remote-filename myBannerFile.txt local-filename /flash0/
myBannerFile.txt default-server

WORKING: TFTP file transfer in progress
t.txt                100%
|********************************************************************|
134   0:00:00 ETA
```

Procedure 4-7
Setting the banners with XML

Update the device’s XML welcome banner file name on the TFTP server for the device. When the XML command file is processed, the welcome banner is sent to the device.

Step	Action
1	Create a text file with the banner text.
2	To manually trigger the command file, enter this command: `software run command-file`

—end—

Example

This example automatically transfers the banner file to the device if DHCP is configured. To manually trigger the command file, enter the software run command-file command.

```
<XmlWwpCommandFile>
     <XmlCmdPlatformClass name="3942"
          version="saos-06-13-00-0187"
          operation="upgrade"
          serviceAffecting="yes">
     </XmlCmdPlatformClass>
     <XmlCmdPlatformClass name="brego"
          configFilePath="myFolder/my-config-file.txt"
          configFileRule="activate"
          welcomeBanner="myBannerFile.txt"
          licenseFile="myLicenseFile.txt"
          version="saos-06-13-00-0187"
          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 4-8
Configuring banners manually

Set the banner files manually to create a customized experience for users.

The login banner is displayed before the user logs in. The welcome banner is displayed after the user logs in.

Step	Action

1 Create text files containing the banner text, such as custom_welcome.txt and custom_login.txt.

2 Ensure you login as a superuser. On user login, the file directory is /tmp/users/username.

3 Transfer the banner files to the 6.x system:

```
system xftp getfile remote-filename <string> local-
filename <string> default-server
```

where

filename <string>	is the name of the custom banner file, such as custom_welcome.txt and custom_login.txt.
default-server	uses the default xFTP server.

For example, to transfer both custom files, enter:

```
system xftp getfile remote-filename custom_welcome.txt
local-filename custom_welcome.txt default-server
```

```
system xftp getfile remote-filename custom_login.txt
local-filename custom_login.txt default-server
```

4 Move the files to a directory where the banner file is stored in flash:

```
mv <banner.txt> <flash_directory>
```

where

<banner.txt>	is the text file used as the banner, such as custom_welcome.txt and custom_login.txt.
<flash_directory>	is the directory where the banner file is stored in flash.

For example, to move both files, enter:

```
mv custom_welcome.txt /flash0/config/
```

```
mv custom_login.txt /flash0/config/
```

5 Determine the banner configuration action that you want to perform.

If you want to	Then
Set the device to use your login banner	Perform step 6.
Reset the login banner to the default values	Perform step 7.
Set the device to use your welcome banner	Perform step 8.
Reset the welcome banner to the default values	Perform step 9.

6 Set the device to use your login banner:

```
system shell banner set banner login filename
<banner.txt>
```

where

<banner.txt>	is the text file used as the banner, such as custom_login.txt.

For example:

```
system shell banner set banner login filename /flash0/
config/custom_login.txt
```

7 Reset the login banner to the default values:

```
system shell banner unset banner login
```

8 Set the device to use your welcome banner:

```
system shell banner set banner welcome filename
<banner.txt>
```

where

<banner.txt>	is the text file used as the banner, such as custom_welcome.txt.

For example:

```
system shell banner set banner login filename /flash0/
config/custom_welcome.txt
```

9 Reset the welcome banner to the default values:

```
system shell banner unset banner welcome
```

—end—

Procedure 4-9
Configuring the banner file

Rather than downloading and manipulating the files, users can create banners directly by typing them into the CLI. Banners created in this way are saved in the config file with all the other settings, and need no special handling.

You can

- collect banner file information
- create a banner with a specific line
- add a line to the banner file
- edit a specified banner
- delete a specified banner
- display the specified banner

Step Action

To collect banner file information

1 Collect banner file information:

```
system shell banner collect {banner <login | welcome>}
```

To create a banner with a specific line

2 Create a banner with a specific line:

```
system shell banner create {banner <login | welcome> line
<STRING>}
```

To add a line to the banner file

3 Add a line to the banner file:

```
system shell banner add {banner <login | welcome> line
<STRING>}
```

To edit a specified banner

4 Edit a specified banner:

```
system shell banner edit {banner <login | welcome>}
```

To delete a specified banner

5 Delete a specified banner:

```
system shell banner delete {banner <login | welcome>}
```

To display the specified banner

6 Display the specified banner:

```
system shell banner show {banner <login | welcome>
```

—end—

Examples

This example creates the banner with the welcome line, “Welcome to SAOS...”

```
system shell banner create banner welcome line “Welcome
to SAOS...”
```

This example adds the banner line “You are welcome here.”

```
system shell banner add banner welcome line “You are
welcome here.”
```

> ***Note:*** The examples shown are for normal mode. For enhanced mode, see “Login banner” on page 11-2.

Procedure 4-10
Clearing login warning banners

The system may issue warning banners at login time to indicate that there were problems in the past. You can clear these banners for future logins. Note that if there are subsequent problems the warning banners return.

This operation is not part of saved configuration: it applies only to the currently running system.

Step	Action
1	Clear a login warning banner: `system shell reset warning-banners`

—end—

Procedure 4-11
Configuring the Guardian software watchdog

When enabled, the Guardian software watchdog restarts the SAOS server process if it appears to be unresponsive and automatically reboots the system if SAOS fails to initialize. In addition, if Guardian detects a critical fault, it collects debug information that can assist Ciena in determining the root cause and providing a resolution to the problem.

You can limit the number of consecutive reboots caused by the Guardian. After three consecutive reboots caused by the Guardian, the Guardian is suspended and does not reboot the system if a deadlock is detected. When the Guardian is in this suspended state, a regular reboot triggers the Guardian to resume normal operation.

Use the `system guardian show` command to view the Guardian administrative and operational states. If one is enabled and the other is disabled, this means that the configuration has been changed, but a reboot has not yet been performed.

> ***Note 1:*** Ciena Engineering strongly recommends that Guardian be left at these default settings:
> — enabled
> — number of consecutive guardian reboots left = no limit
>
> ***Note 2:*** Disabling or limiting Guardian functionality may result in field units becoming "locked up" in an unmanageable state. In the event of an unexpected critical fault, manual intervention (using the front panel reset button) may be required to recover.
>
> ***Note 3:*** Disabling or limiting Guardian functionality may hinder the ability to quickly debug critical field issues.

Step **Action**

To enable Guardian

1 Enable Guardian:

```
system guardian enable
```

To disable Guardian

2 Disable Guardian:

```
system guardian disable
```

To limit the number of consecutive reboots to three

3 Limit the number of consecutive reboots to three:

```
system guardian set limit-number-reboots on
```

To view Guardian configuration details

4 View Guardian configuration details:

```
system guardian show
```

—end—

Example

This example displays Guardian configuration details.

```
+---------------------GUARDIAN---------------------+
| Admin State                        | Disabled    |
| Oper State                         | Enabled     |
| Limit reboots                      | off         |
| Consecutive guardian reboots left  | no limit    |
| Consecutive guardian reboots       | 0           |
| Total guardian Reboots             | 0           |
+------------------------------------+-------------+
```

Procedure 4-12
Displaying system settings

Display system settings to verify the host name, date, and time settings.

You can display time and CPU load by default or with these individual system settings:

- Date
- Host name
- Time
- Time offset
- Up time from last re-boot
- Memory usage

Step **Action**

1 Display all system settings:

```
system show [date] [host-name][memory-usage] [time][time-
offset] [uptime]
```

where

[date]	is the system date.
[host-name]	is the host name of the device.
[memory-usage]	is the system memory usage.
[time]	is the system time.
[time-offset]	is the time-offset in seconds from UTC.
[uptime]	is the system uptime.

—end—

Example

This example displays all system settings.

```
> system show
+------------------------------ HOST NAME -------------------------------+
| Oper  | 3942                                                            |
| User  | 3942                                                            |
| DHCP  |                                                                 |
+-------+-----------------------------------------------------------------+
+---------------------------- TIME Settings -------------------------+
| Parameter                           | Value                        |
+-------------------------------------+------------------------------+
| Local date and time                 | Thu Feb 17 16:46:01 2000     |
| Coordinated Universal Time (UTC)    | Thu Feb 17 16:46:01 2000     |
| Local Time Offset (seconds East)    | 0                            |
| Timestamp                           | Local                        |
+-------------------------------------+------------------------------+
+---------------------------- HEALTH MONITORING ---------------------------+
|              Item                | Health     | Current | Min     | Max     |
|                                  | State      | Value   | Value   | Value   |
+--------------------------------------------------------------------------+
|Cpu Utilization (%)               |            |         |         |         |
| Last 5 seconds                   |     Normal |       8 |       7 |      58 |
| Last 10 seconds                  |     Normal |       9 |       8 |      57 |
| Last 60 seconds                  |     Normal |       9 |       8 |      30 |
+--------------------------------------------------------------------------+
|Cpu Load Average                  |            |         |         |         |
| Last 1 minute                    |     Normal |    0.19 |    0.02 |    1.18 |
| Last 5 minutes                   |     Normal |    0.25 |    0.10 |    0.54 |
| Last 15 minutes                  |     Normal |    0.21 |    0.06 |    0.32 |
+--------------------------------------------------------------------------+
|Memory Utilization (Kbytes)       |            |         |         |         |
| Used                             |        n/a |  249060 |  243172 |  252988 |
| Available                        |     Normal |  750860 |  746932 |  756748 |
+--------------------------------------------------------------------------+
|File System Utilization (% usage) |            |         |         |         |
| /tmp/                            |     Normal |       0 |       0 |       0 |
| /mnt/sysfs/                      |     Normal |       4 |       4 |       4 |
+--------------------------------------------------------------------------+
+----------------------GUARDIAN---------------------+
| Admin State                        | Enabled      |
| Oper State                         | Enabled      |
| Limit reboots                      | off          |
| Consecutive guardian reboots left  | no limit     |
| Consecutive guardian reboots       | 0            |
| Total guardian Reboots             | 0            |
+------------------------------------+--------------+

+--------------- SYSTEM SERVERS ------------------+
| Server | Admin State          | Oper State      |
+--------+----------------------+-----------------+
| SFTP   | Disabled             | Disabled        |
+--------+----------------------+-----------------+
```

Procedure 4-13
Displaying the system shell attributes

Display the system shell attributes to verify the inactivity timer, lines to display, and welcome banner settings.

Step **Action**

To display the shell settings

1 Display the system shell settings:

```
system shell show
```

To display the banner file configuration

2 Display the banner file configuration:

```
system shell banner show <login|welcome>
```

To display the shell system configuration

3 Display the shell system configuration:

```
system shell session show
```

—end—

Example

This example shows sample output for the system shell show command.

```
system shell show
+------------------------ Shell Settings -----------------------+
| Parameter                   | Value                           |
+-----------------------------+---------------------------------+
| Global more                 | on                              |
| Global more lines           | 0                               |
| Global inactivity timer     | off                             |
| Global inactivity timeout   | 1500 min                        |
| Global login timer          | off                             |
| Global login timeout        | 60 sec                          |
| More (session)              | On                              |
| More lines (session)        | 0                               |
| Window width (session)      | 80                              |
| Window height (session)     | 25                              |
| Login banner file           | (none)                          |
| Welcome banner file         | (none)                          |
+-----------------------------+---------------------------------+
```

This example shows sample output for the system shell session show command.

```
> system shell session show

+------------------------------- SHELL SETTINGS --------------------------------+
| Parameter                    | Value                                          |
+------------------------------+------------------------------------------------+
| More (session)               | On                                             |
| More lines (session)         | 0                                              |
| TAB-More (session)           | On                                             |
| Window width (session)       | 80                                             |
| Window height (session)      | 25                                             |
+------------------------------+------------------------------------------------+
```

Procedure 4-14
Disabling and enabling the RADIUS/TACACS login authentication message

You can disable and enable the default message, “Waiting for authentication server reply” displayed to users while the system is authenticating their submitted RADIUS or TACACS credentials.

Step **Action**

To disable the message

1 Enter this command:

```
system shell set login-authentication-message off
```

To enable the message

2 Enter one of these commands:

```
system shell set login-authentication-message on
```

OR

```
system shell unset login-authentication-message
```

Procedure 4-15
Clearing configuration failure warnings

When a configuration file appears to have caused a crash or it cannot be properly executed, messages about the problem are displayed to users when they log on to the system.

- This message is displayed when the configuration file appears to have caused a crash:

```
### WARNING ###
SAOS seems to have crashed last time as a result of the saved
system configuration, so this time the configuration has not
been restored.
Check the event log “log flash view” for a detailed list of
problems found.
### WARNING ###
```

- This configuration failure message is displayed if one or more lines in the configuration file fail:

```
### WARNING ###
One or more problems occurred while attempting to restore
system configuration at startup. Check the event log
("log flash view") for a detailed list of problems found.
### WARNING ###
```

Even if the configuration errors are addressed, these warning messages continue to be displayed until a system reboot or until they are explicitly cleared.

Use this procedure to clear specific messages.

Step **Action**

To cancel a “no restored” warning

1 Enter this command:

```
configuration clear no-config-warning
```

To cancel a “configuration errors during restore” warning

2 Enter this command:

```
configuration clear config-errors-warning
```

—end—

System access

This section provides the procedures needed to access the system:

Procedure 5-1
Accessing the CLI using Telnet or SSH

To access the device through Telnet or SSH

- the device must have an IP address
- the Telnet or SSH version 2 (v2) client must have a route set up to allow access to the device
- the user must have a valid user name and password to log in.

The Security license must be installed to use SSH.

- For information on SSH, see "SSH" on page 10-1.
- For information on licenses, refer to *39XX/51XX Software Management and Licensing*.

All devices coming out of manufacturing have their local interface configured to use IP address 172.16.233.214. This IP address must be used when connecting to a device that has not gone through a DHCP process.

If the device has gone through the DHCP process, the DHCP server assigns an IP address based on the device's MAC address.

Step **Action**

1 Determine the IP address for the device.

2 Obtain a valid user name and logon password.

3 Configure default gateway setup to access the device.

4 Use a Telnet or SSH v2 client to connect to the device.

5 At the logon prompt, enter a user name and then a password to access the prompt, for example:

```
3903 login: su
Password:


SAOS is True Carrier Ethernet TM software.
Welcome to the shell
3903>
```

—end—

Procedure 5-2
Accessing the CLI using the serial console port

By default, the serial console port is enabled.

For cable part numbers, refer to *39XX/51XX Planning, Engineering and Ordering*.

1 Connect a terminal or PC running terminal emulation software to the serial console port using a null modem cable.

Note: The serial console port does not support connectivity to a modem.

2 Configure the connected terminal with these settings:

- Character size = 8
- Parity = None
- Stop Bit = 1
- Rate = 9600 bps
- Control = None

3 At the logon prompt, enter a user name and then a password to access the prompt, for example:

```
3903 login: su
Password:


SAOS is True Carrier Ethernet TM software.
Welcome to the shell
3903>
```

—end—

Procedure 5-3
Logging on as a different user

You can log on with a different user name without disconnecting your Telnet session.

Step	Action
1	Log on as a different user: `user relogin-as user <Username String[32]>`

—end—

Example

This example logs the user on as superuser.

```
user relogin-as user su
```

Procedure 5-4
Establishing the console-port connection to an NFV Server module

If a 39x6 system includes an NFV Server module, use this procedure to establish the console-port connection to the module.

The console connection to the module can be established after the module has booted up and has been detected by the 39x6. If the module does not fully boot or if it is not detected by the 39x6, then you can use the force option to establish a connection.

Step	Action

Establish a console-port connection to the NFV Server module

1 Open a connection to the module:

```
module diag-shell module <module>
```

where

module <module>	is the module name.

Note: Note: If the module is not detected, the system will issue an error message.

Establish a console-port connection to the NFV Server module using the force option

If the x86 NFV Server module is not detected by the 39x6, use the force option to force a connection to the module:

```
module diag-shell module NFV force
```

This connects to the diag shell even if the module is not present, and gives the diag information. When the module is inserted, a connection will be made to the module's diag shell.

—end—

Data collection configuration and management

This section provides the procedures needed to perform data collection configuration and management:

Statistics attribute

This table lists the values for the statistics attribute, which selects the statistics to be collected and stored.

Table 6-1
Values for the statistics attribute

Value	Description
basicError	Default selection includes: • portRxCrcErrorPkts • portUndersizePkts • portOversizePkts • portFragmentsPkts • portJabbersPkts • portDropEvents • portTxCrcErrorPkts • portTxCollPkts
basicRx	Default selection includes: • portRxBytes • portRxPkts • portRxMcastPkts • portRxBcastPkts
basicTx	Default selection includes: • portTxBytes • portTxTBytes • portTxPkts • portTxBcastPkts • portTxMcastPkts

Table 6-1
Values for the statistics attribute

Value	Description
errorAll	Optional selection includes: • portTxExDeferPkts • portTxGiantPkts • portTxUnderRunPkts • portTxLCheckErrorPkts • portTxLOutRangePkts • portTxLateCollPkts • portTxExCollPkts • portTxSingleCollPkts • portTxCollPkts • portInDiscards • portTxPausePkts • portRxPausePkts • portTxDeferPkts • portRxLOutRangePkts

Table 6-1
Values for the statistics attribute

Value	Description
rxAll	Optional selection includes all basicRx statistics plus the following: • port64OctsPkts • port65To127OctsPkts • port128To255OctsPkts • port256To511OctsPkts • port512To1023OctsPkts • port1024To1518OctsPkts • portRx1519To2047OctsPkts • portRx2048to4095OctsPkts • portRx4096to9216OctsPkts • portRxUcastPkts
txAll	Optional selection includes all basicTx statistics plus the following: • portTx64OctsPkts • portTx65To127OctsPkts • portTx128To255OctsPkts • portTx256To511OctsPkts • portTx512To1023OctsPkts • portTx1024To1518OctsPkts • portTx1519To2047OctsPkts • portTx2048to4095OctsPkts • portTx4096to9216OctsPkts • portTxUcastPkts
standard	Optional selection includes all basicRx, basicTx, basicError and these statistics from the RMON MIB: • etherHistoryUtilization • etherHistoryHighCapacityOverflowPkts • etherHistoryHighCapacityOverflowOctets

Procedure 6-1
Configuring an RMON history group

Configure a history group to monitor and store port Ethernet statistics.

The number of history entries depends upon the switch as shown in this table.

Table 6-2
Number of history entries for each switch

Platform	Number of History Entries
3903, 3903x	3
3904	6
3905	6
3906	3
3926	30
3928	30
3942	30
5142	30
5160	30

A bucket is one sample of data collection during a distinct time interval.

You can

- create an RMON history entry
- set an RMON history attribute
- unset an RMON history attribute
- delete a history entry

Step **Action**

To create an RMON history entry

1 Create an RMON history entry:

```
rmon history add hist-index <NUMBER: 1..65535> [file-
logging <on|off>] port <Port> [interval <duration:
{N[yMwdhms]} *e.g. 1h10m3s>] [num-buckets <NUMBER:
1..x65535>] [owner <String[1..127]>][sample-type
<absolute | delta>] [statistics <basicError | basicRx |
basicTx | errorAll | rxAll | txAll | standard>]
```

where

hist-index <number: 1..65535>	is the index in the history table.
file-logging <on | off>	enables or disables saving the history to a file. The default value is off.
port <logical-port>	is the port.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s>]	is the interval to be used for monitoring history statistics, 1sec to 1hr (N[yMwdhms]...). The default value is 1800 seconds.
num-buckets <NUMBER:1-65535>	is the number of buckets to use. The default value is 50.
owner <String[1..127]>	is the name of the owner of the history entry. The default value is blank.
sample-type <absolute | delta>	is the absolute or delta for the sample. The default is absolute.
statistics <basicError | basicRx | basicTX | errorAll | rxAll | txAll | standard	sets the type of statistics.

To set an RMON history attribute

2 Set an RMON history attribute:

```
rmon history set hist-index <NUMBER: 1..65535> [file-
logging <on|off>] {port <Port>} [interval <duration:
{N[yMwdhms]} *e.g. 1h10m3s>][num-buckets <NUMBER:
```

```
1..65535>] [owner <String[1..127]> [sample-type <absolute
| delta>] [statistics <basicError | basicRx | basicTx |
errorAll | rxAll | txAll | standard>]
```

where

hist-index <NUMBER: 1..65535>	is the history index.
file-logging <on | off>	enables or disables saving the history to a file. The default value is off.
port <Port>	is the port.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s>]	is the interval to be used for monitoring history statistics, 1sec to 1hr (N[yMwdhms]...). The default is 1800.
num-buckets <NUMBER:1..65535>	is the number of buckets to use. The default value is 50.
owner <String[1..127]>	is the name of the owner of the history entry. The default value is blank.
sample-type <absolute | delta>	is the absolute or delta for the sample. The default is absolute.
statistics <basicError | basicRx | basicTX | errorAll | rxAll | txAll | standard	sets the type of statistics.

To unset an RMON history attribute

3 Unset an RMON history attribute:

```
rmon history unset hist-index <NUMBER: 1..65535> [file-
logging] [interval] [num-buckets] [owner] [sample-type]
[statistics]
```

where

hist-index <NUMBER: 1..65535>	is the index in the history table.
file-logging	enables or disables saving the history to a file. The default value is off.
interval	is the interval used for monitoring. The default value is 1800.
num-buckets	is the number of buckets to use. The default value is 50.

where

owner
is the name of the owner of the history entry. The default value is blank.

sample-type <absolute | delta>
is the absolute or delta for the sample. The default is absolute.

statistics <basicError | basicRx | basicTX | errorAll | rxAll | txAll | standard
sets the type of statistics.

To delete a history entry

4 Remove an Ethernet statistics history entry:

```
rmon history remove hist-index <NUMBER: 1..65535>
```

where

hist-index <NUMBER: 1..65535>
is the index of the created entry in the history table.

—end—

Example

This example manually adds an entry for port 3.

```
> rmon history add histindex 3 interval 1800 num-buckets 1050 owner Admin file-
logging on sample-type delta statistics rxAll
```

This example displays history entries.

```
> rmon show history

+-------------------------------RMON HISTORY STATISTICS------------------------------------------------+
| Index  | Port    | OID             | Requested | Granted  | Interval| Owner| File| Sample  | Statistics|
|        |         |                 | Buckets   | Buckets  |         |      |     |         |           |
+--------+---------+-----------------+-----------+----------+---------+------+-----+---------+-----------+
| 3      | 3       | ifIndex.10003   | 1050      | 1050     | 1800    | Admin| On  | delta   | rxAll     |
+--------+---------+-----------------+-----------+----------+---------+------+-----+---------+-----------+
```

This example deletes a history event with an index of 1.

```
> rmon history remove hist-index 1
```

Procedure 6-2
Configuring RMON automatic history entries

You can

- set global RMON history settings
- unset RMON history settings
- enable RMON history auto-configuration
- disable RMON history auto-configuration

Step **Action**

To set global RMON history settings

1 Set global RMON history settings:

```
rmon history auto-configure set interval [<duration:
{N[yMwdhms]} *e.g. 1h10m3s>] [num-buckets <NUMBER:1-
65535>] [owner <String[1..127]>] [file-logging <on|off>]
[statistics <basicError | basicRx | basicTx | errorAll |
rxAll | txAll | standard>]
```

where

interval <duration: {N[yMwdhms]} *e.g. 1h10m3s>]	is the interval to be used for monitoring history statistics, 1sec to 1hr (N[yMwdhms]...). The default is 1800.
num-buckets <NUMBER:1-65535>	is the number of buckets to use. The default value is 4 for automatically-configured entries.
owner <String[1..127]>	is the name of the owner of the history entry. The default value is “Auto Generated” for automatically-configured entries.
file-logging <on | off>	enables or disables saving the history to a file. The default value is on for automatically-configured entries.
statistics <basicError | basicRx | basicTX | errorAll | rxAll | txAll | standard	sets the type of statistics.

To unset RMON history settings

2 Configure RMON auto-configuration:

```
rmon history auto-configure unset [interval] [num-
buckets] [owner] [file-logging] [statistics]
```

where

interval	is the interval used for monitoring.
num-buckets	is the number of buckets to use. The default value is 4 for automatically-configured entries.
owner	is the name of the owner of the history entry. The default value is “Auto Generated” for automatically-configured entries.
file-logging	enables or disables saving the history to a file. The default value is on for automatically-configured entries.
statistics	identifies which per port statistics to place in the file. See the list of Values for the statistics attribute for more information.

To enable RMON history auto-configuration

3 Enable RMON history auto-configuration:

```
rmon history auto-configure enable
```

To disable RMON history auto-configuration

4 Disable RMON history auto-configuration:

```
rmon history auto-configure disable
```

—end—

Example

This example configures automatic history entries.

```
rmon history auto-configure enable
```

Procedure 6-3
Configuring user history

Configure user history to specify the MIB information to be collected. When configuring user history, you need to define an SNMP object along with an optional control entry.

You can

- add a user history object
- add a user history table entry
- change a user history table entry
- unset a user history table entry
- remove a control table entry

Step **Action**

To add a user history object

1 Add a user history object:

```
rmon usr-history add usr-index <NUMBER: 1..65545>
control-index <NUMBER: 1..1200> object <String[1..127]>
sample-type <absolute|delta>}
```

where

usr-index <1..65545>	is the index in the user history object table.
control-index <1..1200>	is the index of history control table to associate with.
object <String[1..127]>	is the OID name.
sample-type <absolute|delta>	is the absolute or delta for sample. The default value is absolute.

To add a user history table entry

2 Add a user history table entry:

```
rmon usr-history add control-index <NUMBER: 1..1200> usr-
index <NUMBER: 1..65545> [buckets <NUMBER: 1..65535>]
[file-logging <on|off>] [interval <duration: {N[yMwdhms]}
*e.g. 1h10m3s>] [owner <String[1..127]>]
```

where

control-index <NUMBER: 1..1200>	is the index of history control table to associate with.
usr-index <NUMBER: 1..65545>	is the index of the user-history object table to associate with.
[buckets <NUMBER: 1..65535>]	is the number of buckets to use.
file-logging <on | off>	enables or disables saving the history to a file.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s>]	is the interval to be used for monitoring usr-history objects, 1sec to 1y (N[yMwdhms]...).
owner <String[1..127]>	is the name of the owner of the history entry.

To change a user history table entry

3 Change a user history table entry:

```
rmon usr-history set control-index <control-index>
[buckets <NUMBER: 1-65535>] [file-logging <on|off>]
[interval <duration: {N[yMwdhms] *e.g. 1h10m3s>] [owner
<String[1..27]>]
```

where

control-index <control-index>	is the index of history control table to associate with
[buckets <NUMBER: 1-65545>]	is the number of buckets to use.
file-logging <on | off>	enables or disables saving the history to a file.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s>]	is the interval to be used for monitoring usr-history objects, 1sec to 1y (N[yMwdhms]...).
owner <String[1..127]>	is the name of the owner of the history entry.

To unset a user history table entry

4 Unset a user history table entry:

```
rmon usr-history unset control-index <control-index>
[buckets] [file-logging] [interval] [owner]
```

where

control-index <control-index>	is the index of history control table to associate with
buckets	is the number of buckets to use.
file-logging	enables or disables saving the history to a file.
interval	is the interval used for monitoring, in seconds.
owner	is the name of the owner of the history entry.

To remove a control table entry

5 Remove a control table entry:

```
rmon usr-history remove [control-index <NUMBER: 1-1200>]
[usr-index <NUMBER 1-6400>]
```

where

control-index <NUMBER: 1-1200>	is the index of the history control table to associate with.
usr-index <NUMBER:1-65545>	is the index in the user history object table.

—end—

Example

This example adds a user history object entry.

```
rmon usr-history add usr-index 6000 control-index 1000
object 125 sample-type delta
```

This example adds a user history control entry.

```
rmon history add index 1
```

This example deletes an history object entry.

```
rmon usr-history remove control-index 1 usr-index 1
```

This example deletes the specified history control entry.

```
rmon usr-history remove control-index 1
```

Procedure 6-4
Configuring RMON file settings

RMON allows you to

- maintain persistent history and user history files
- transfer files to a server

To make the history persistent, you need to enable file logging when adding the history entry, and then create an entry for the file.

After the file persistence settings are configured, you can change the settings. Only changes to the interval and state take effect immediately. All other changes do not take effect until the interval is complete. Local files are located in /flash1/log and are named rmonHistory.x. Integer x increases each time the file is written.

You can

- configure RMON file settings
- unset RMON file settings
- enable RMON file transfer
- disable RMON file transfer
- push all RMON files on the device to the server

  Note: Default server settings are made using the system xftp set command, as described in *Software Management and Licensing* in the section on managing system software.

Step **Action**

To configure RMON file settings

1 Configure RMON settings:

```
rmon transfer set {filename <String>}
{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

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use 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 sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

To unset RMON file settings

2 Unset RMON file settings:

```
rmon transfer unset [name] [interval] [num-files]
[remote-file-dir] {tftp-server} {ftp-server} {sftp-
server} [server]
```

where

name	name of RMON file
interval	interval used for monitoring
num-files	interval used for monitoring
remote-file-dir	remote file directory
tftp-server	unset TFTP server
ftp-server	unset FTP server
sftp-server	unset SFTP server
server	server

To enable RMON file transfer

3 Enable RMON file transfer:

```
rmon transfer enable
```

To disable RMON file transfer

4 Disable RMON file transfer:

```
rmon transfer disable
```

To push all RMON files on the device to the server

5 Push all RMON files on the device to the server:

```
rmon transfer push
```

—end—

Procedure 6-5
Displaying RMON information

You can display

- RMON history information
- file persistence settings and the status of file transfers
- user history object and control entries
- history statistics
- auto-configuration history
- RMON history
- alarm history
- event history

Step **Action**

To display RMON history information

1 Display RMON history information:

```
rmon show history
```

To display file persistence settings and the status of file transfers

2 Display file persistence settings and the status of file transfers:

```
rmon show transfer
```

To display user history object and control entries

3 Display user history object and control entries:

```
rmon show user-history
```

To display history statistics

4 Display history statistics:

```
rmon show statistics
```

To display RMON auto-configuration history

5 Display RMON auto-configuration history:

```
rmon show auto-configuration
```

To display RMON alarm history

6 Display RMON alarm history:

```
rmon show alarm
```

To display RMON event history

7 Display RMON event history:

```
rmon show event
```

—end—

Example

This example shows sample output for the rmon show user-history command.

```
> rmon show user-history

WARNING: This CLI output may take few minutes depending on the number of entries

+---------------------------- RMON USR-HISTORY CONTROL TABLE --------------------------+
| Index | Object | Requested| Granted | Interval (sec)   | Owner           | File| Bins|
|       |        | Buckets  | Buckets |                  |                 | Log | Used|
+-------+--------+----------+---------+------------------+-----------------+-----+-----+
|     1 |      2 |         4|       4 | 15s          (15)| usrHistory      | yes |    8|
+-------+--------+----------+---------+------------------+-----------------+-----+-----+

+----------------------- RMON USR-HISTORY OBJECT TABLE ----------------------+
| Object | Control|                 Data Source                   | Sample   |
| Index  | Index  |                                               | Type     |
+--------+--------+-----------------------------------------------+----------+
|     20 |      1 | wwpLeosPortTotalStatsRxBytes.1                | Absolute |
|     21 |      1 | wwpLeosPortTotalStatsTxBytes.1                | Absolute |
+--------+--------+-----------------------------------------------+----------+
```

Procedure 6-6
Displaying system processes

Display system processes when troubleshooting.

Step **Action**

1 Display system process information:

```
system ps show [format <wide>]
```

where

format <wide> is the format of the display.

—end—

Example

This example shows sample output for the system ps show command.

```
> system ps show
PID TTY          TIME CMD
1945 pts/0    00:00:01 main_1945
1947 pts/0    00:00:00 leos
2995 pts/0    00:00:00 more
2996 pts/0    00:00:00 ps
```

Procedure 6-7
Generating a system state dump file

For troubleshooting purposes, you can generate a system state dump file to transfer to an xFTP server. The state dump file contains configuration and status information for major device components all in one file, including:

- system configuration
- interface configuration
- chassis device identification, device archives, and power supplies
- module configuration, temperature, CPU load, and POST
- port configuration and status
- system process information
- configuration file
- log files
- optional datapath information
- optional core files

The state dump information also includes IPv6 interface configuration information.

> ***Note 1:*** Default server settings are made using the system xftp set command, as described in 39XX/51XX Switches and Platforms Software Management and Licensing in the section on managing system software.
>
> ***Note 2:*** The system allows only one state dump collection at a time.

Step **Action**

1 Generate a system state dump file:

```
system state-dump {filename <String>}
{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

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use 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 sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

Example

This example shows sample output for the system state-dump command.

```
> system state-dump file-name dump.tgz ftp-server 10.25.35.12
Testing access to remote file dump.tgz

WORKING: FTP file transfer in progress

Writing system info
Writing interface info
Writing software info
Writing FPGA info
Writing chassis info

Writing port info
Writing Transceiver info
Writing Device Archive
Writing health info
Writing fan info
Writing SecLog stats
Writing alarm info
Writing DHCP info
Writing Configuration Settings
Writing running system configuration
Writing OSE Emulation Process Listing
Writing Process Listing
Writing Core file list
Writing fib/aib, static ARP info
Writing fib Sinar list
Writing MPLS tunnel info
Writing MPLS l2-vpn info
Writing MPLS mpg info
Writing ARP info
Writing CFM global info
Writing RAPS info
Writing RAPS Logical ring info
Writing RAPS Virtual ring info
Writing Aggregation info
Writing LLDP info
Writing LLDP show neighbors info
Writing AIS information
Writing Filesystem layout
Gathering SAOS log files
Writing RAM log files
Gathering Diagnostic shell log files
Gathering Syslog files
Gathering config files
Writing BFD Session info
Writing BFD Interface Blade info
Writing iptables (firewall) info
Writing lsof -i4 -i6 info
Writing frame handlers - manager
Writing OSE emulation status
Writing parameters (aka cookies)
Writing Shell completion tables
Gathering evt logs
Writing evt log reports
Writing Attached Files
Writing End of State Dump
Building tar file
Ready to transfer to remote file dump.tgz
WORKING: FTP file transfer in progress
File dump.tgz transferred to FTP server 10.25.35.12
Removing state-dump residue in /tmp/temp1918.0.d
State-dump finished
```

The example above uses the default server as configured by the system xftp set command:

```
system xftp set ftp-server <IpHost>
system xftp set ftp-server <IpHost> login-id <String>
system xftp set ftp-server <IpHost> echoless-password
system xftp set tftp-server <IpHost>
system xftp set sftp-server <IpHost>
system xftp set sftp-server <IpHost> login-id <String>
system xftp set sftp-server <IpHost> echoless-password
system xftp set mode <ftp|sftp|tftp>
```

This example uses the default SFTP server.

```
> system state-dump default-sftp-server file-name test-state-dump
Writing system info
Writing software license info
Writing interface info
Writing chassis info
Writing module info
Writing port info
Writing archive info
Writing system config
Writing log files
Writing evt logs
WORKING:: SFTP file transfer in progress
File test-state-dump transferred to xftp server 10.5.4.16
```

Security fundamentals

Security features are employed to prevent unauthorized access to network resources and to deployed services to control the way that services are distributed through the network. Some features restrict certain types of protocols or packets, while others restrict port access.

Users have Telnet, SSH, or serial console access to the CLI through user accounts. When logging in, users are asked to supply a user name and password. If users do not supply the correct password, or if the user account does not exist, the system denies access. When creating a user account, the password can be specified as echoless or as encrypted. Encrypted passwords are designed to be extremely difficult to view in the clear.

Controlling device access through user accounts enables the network operator to expressly define those users that can view configuration information and those that can view and modify configuration information.

When a user account is created, it is assigned a privilege level.

These sections discuss security on 39XX/51XX switches:

- "User configuration and management" on page 8-1
- "User and user access security" on page 9-1
- "Secure communications and infrastructure" on page 10-1
- "Performing security containment and recovery" on page 13-1

User configuration and management

As described in “Administration fundamentals”, some default users exist. This section details the commands used to configure and manage user accounts.

User accounts

A user at the super user access level can create user accounts with these access levels:

- limited (read-only)
- admin (read/write)
- superuser (read/write)
- diag (read/write/diagnostic)

User names and passwords are case sensitive. User names are limited to a length of 32 characters and passwords are limited to a length of 128 characters. When creating a user account, the password can be specified in the clear (but using a traditional blind double-entry-with-verification collection mechanism so that the password cannot be readily observed). When these passwords are entered by means of an SSH session, a cleartext password is never visible anywhere at any time, including over the network. A user account can also be created without a password, although Ciena does not recommend this.

You can also configure password character options for user accounts.

> ***Note:*** TACACS+ and RADIUS also allow user names of up to 32 characters and passwords of up to 128 characters.

To enhance password security, these password rules are strongly recommended:

- a minimum length of eight characters
- a minimum of one lower case letter, one upper case letter, one number and one special character
- no repeated consecutive characters
- no dictionary words, names or telephone numbers.

These rules can be enforced by a super user via the password character options.

When you create user accounts and save the configuration, the user create user command is saved in the SECURITY CONFIG: section of the configuration file. The clear text password is saved in a hashed form, although the user logs on using the original clear text password.

> ***Note:*** If a user is authenticated by means of RADIUS or TACACS+, you cannot create the same local user by means of CLI commands while the user is logged in. An error message indicates that the account already exists even though it is not listed in the “user show” output. The local account cannot be created until all sessions of that user log off.

Controlling device access through user accounts enables the network operator to expressly define those users that can view configuration information and those that can view and modify configuration information.

In addition to the CLI, it is also possible to modify password policy using SNMP. This capability is disabled by default, and must be enabled through the CLI. Instructions on enabling password policy modification through SNMP are provided in the procedures.

If a user password is forgotten, it cannot be retrieved. A superuser can assign the user a new password or the user can be deleted and added again with a different password.

User lockout-policy

SAOS users with super level privileges can enable a lockout policy on user accounts. This means that when the user hits a set level of login failures, the account is locked and any additional logins are prevented until the lockout period has expired. The super user can configure the lockout period and the number of failures that are required for a lockout to go into effect. The super user can also reset a user’s locked out status through the reset portion of the user lockout menu.

The user lockout policy does not affect any users on the serial console, even locked accounts, as to prevent any possible denial of service and always allows a user to get access to the device. The user lockout policy only affects remote logins using local authentication. This means that users logging in through protocols such as RADIUS are excluded from the lockout policy.

Once an account is locked out, the user is locked out for the set lockout time which is reset to the full duration on any further attempts on the account. When that time has expired, the user is allowed a single attempt at logging in which, if failed, locks the account again.

Procedures are:

- “Creating a user account” on page 8-4
- “Setting the maximum server connections” on page 8-6
- “Modifying a user account” on page 8-7
- “Configuring the minimum user name length for user accounts” on page 8-8
- “Displaying the minimum user name length for user accounts” on page 8-9
- “Configuring the password character options for user accounts” on page 8-10
- “Resetting the password character options for user accounts” on page 8-13
- “Displaying the current user password policy settings” on page 8-15
- “Enabling SNMP password policy modification capability” on page 8-16
- “Enabling and disabling user lockout-policy” on page 8-17
- “Configuring the user lockout-policy” on page 8-18
- “Resetting the user lockout-policy” on page 8-19
- “Displaying the user lockout-policy” on page 8-20

Procedure 8-1
Creating a user account

Create a user account. You can specify one of these passwords:

- echoless-password
- no password

Step **Action**

1 Create a user account:

```
user create user <String>
access-level <limited|admin|super|diag> [echoless-
password]| [nopassword]|
```

where

user <String>	is the user name for the account
[access-level <limited|admin|super|diag>],	is the access level for the user account
[echoless-password]	engages an echoless password collector.
no password	indicates that the user account does not require a password.

2 Determine the password requires for the user account:

If you selected	Then

echoless-password	The system prompts you to enter a password which does not display as you type:
	`Enter Password:`
	Verify the password string you typed. Again, the password does not display as you type:
	`Verify Password:`

nopassword	Press Enter after you select the access-level.

3 Display the accounts in the system:

```
user show
```

4 Repeat step 1 and step 2 for every remaining user account you want to create.

5 When you are finished creating user accounts, save and complete the process:

```
configuration save
```

—end—

Example

This example creates a super user account, MIS, with an cleartext password:

```
user create user MIS access-level super echoless-password
```

This example creates a diag user account, user1, with no password.

```
user create user user1 access-level diag
```

Procedure 8-2
Setting the maximum server connections

Set the maximum server connections for each privilege level.

Step	Action
1	Set the maximum server connections for each privilege level:

```
user set user <user> {[max-limited-users <NUMBER: 0..9>]
[max-admin-users <NUMBER: 0..10>] [max-super-users
<NUMBER: 1..10>]
```

where

user <user>	is the user that you are setting the maximum server connections for.
max-limited-users <NUMBER: 0..9>	sets the maximum simultaneous limited user logins
max-admin-users <NUMBER: 0..10>	sets the maximum simultaneous admin user logins.
max-super-users <NUMBER: 1..10>	sets the maximum simultaneous super user logins.

—end—

Example

This example sets the maximum number of users for the user groups limited, admin and super:

```
user set user1 max-limited-users 5 max-admin-users 6 max-
super-users 8
```

Procedure 8-3
Modifying a user account

Set the access level for a user account to define the privileges of the user.

Step **Action**

1 Set the access level for a user account:

```
user set user <user> {access-level
<limited|admin|super|diag>} [echoless-password]
{nopassword}
```

where

<user>	is the user account that you want to set the access level for
access-level <limited|admin|super|diag>	is the access level
echoless-password	collect user password interactively.
nopassword	no password.

Note: If you use the echoless-password option, you are prompted to enter your password, which is not displayed on the screen. You are then prompted to verify the password. Again, the password does not display on the screen.

2 When you are finished modifying the user account(s), save and complete the process:

```
configuration save
```

—end—

Procedure 8-4
Configuring the minimum user name length for user accounts

Configure the minimum length in characters of user names.

> ***Note:*** If any existing user names are less than the minimum length entered, a warning message is displayed indicating how many existing user names have lengths below the entered limit, and that these user names must be deleted before the new minimum character limit can be set.

Step **Action**

1 Configure the minimum length of user names for user accounts:

```
user username-policy set min-length <NUMBER: 1..32>
```

where

min-length <NUMBER: 1..32>	is the minimum length of the password in characters. The default value is 0 which indicates that there is no minimum.

—end—

Example

This example attempts to set the minimum length of user names to 5 characters. User names shorter than this already exist, and the new limit is rejected:

```
>user username-policy set min-length 5
There are 7 username(s) less than the 5 character minimum.
Please remove all accounts with usernames less than the minimum.
ERROR: Minimum username length could not be set
```

This example sets the minimum length of user names to 4. The new minimum is accepted.

```
user username-policy set min-length 4
```

Procedure 8-5
Displaying the minimum user name length for user accounts

Display the minimum length in characters of user names.

Step **Action**

1 Display the minimum length of user names for user accounts:

```
user username-policy show
```

—end—

Example

This example displays the current minimum length setting for the user name policy:

```
user username-policy show
```

```
+------------- USERNAME POLICY SETTINGS --------------+
| Setting                                | Value      |
+----------------------------------------+------------+
| Minimum Length                         | 4          |
+----------------------------------------+------------+
```

Procedure 8-6
Configuring the password character options for user accounts

This command configures:

- if dictionary words can be used in passwords
- if the user name or its reverse can be used in the associated account password
- the minimum number of upper case, lower case, numeric, special and total characters in account passwords
- the maximum number of times a character can be consecutively repeated in a password
- when changing passwords, the minimum number of characters that must differ from those in the same position in the old password

The minimum length of the password must be greater than the sum of the uppercase, lowercase, numeric and special characters.

Step **Action**

1 Configure the minimum number of password character options for user accounts:

```
user password-policy set [disallow-dict-words <on|off>]
[disallow-username <on|off>] [max-repeated-chars
<NUMBER: 0..128>] [min-character-change <NUMBER: 0..128>]
[min-length <NUMBER: 0..128>] [min-lowercase-chars
<NUMBER: 0..128>] [min-numeric-chars <NUMBER: 0..128>]
[min-special-chars <NUMBER: 0..128>] [min-uppercase-
chars <NUMBER: 0..128>]
```

where

disallow-dict-words <on|off>
allows or disallows dictionary words in a password. The default value is off.

disallow-username <on|off>
allows or disallows passwords to contain the account user name or its reverse. The default value is off.

max-repeated-chars <NUMBER: 0..128>
is the maximum number of characters that can be consecutively repeated. The default value is 0 which indicates that there is no maximum.

where

min-character-change <NUMBER: 0..128> is the minimum number of characters that must differ from those in the same position when the password is changed. The default value is 0 which indicates that there is no minimum.

min-length <NUMBER: 0..128> is the minimum length of the password in characters. The default value is 0 which indicates that there is no minimum.

Values of 1, 2, 3 and 4 are not accepted.

min-lowercase-chars <NUMBER: 0..128> is the minimum number of lowercase characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

min-numeric-chars <NUMBER: 0..128> is the minimum number of numeric characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

min-special-chars <NUMBER: 0..128> is the minimum number of special characters that passwords must contain. The default value is 0 which indicates that there is no minimum. See “Changing a password for a user account” on page 13-7 to understand which special characters are permitted.

min-uppercase-chars <NUMBER: 0..128> ts the minimum number of uppercase characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

—end—

Example

This example sets these password attributes:

- dictionary words are not allowed (default)
- user names cannot be used in passwords (default)
- a character can be consecutively repeated a maximum of 2 times
- the minimum number of characters that must change between password changes is 5
- the minimum password length is 8 characters
- at least 1 lowercase character must be used
- at least 1 numeric character must be used
- at least 1 special character must be used
- at least 1 uppercase character must be used

```
user password-policy set max-repeated-chars 2 min-
character-change 5 min-length 8 min-lowercase-chars 1 min-
numeric-chars 1 min-special-chars 1 min-uppercase-chars 1
```

Procedure 8-7
Resetting the password character options for user accounts

Reset the password policy settings to their default values.

Step **Action**

1 Configure the minimum number of password character options for user accounts:

```
user password-policy unset [disallow-dict-words]
[disallow-username] [max-repeated-chars] [min-character-
change] [min-length] [min-lowercase-chars] [min-numeric-
chars] [min-special-chars] [min-uppercase-chars]
```

where

disallow-dict-words — allows or disallows dictionary words in a password. The default value is off.

disallow-username — allows or disallows passwords to contain the account username or its reverse. The default value is off.

max-repeated-chars — is the maximum number of characters that can be repeated. The default value is 0 which indicates that there is no maximum.

min-character-change — is the minimum number of characters that must differ from those in the same position when the password is changed. The default value is 0 which indicates that there is no minimum.

min-length — is the minimum length of the password in characters. The default value is 0 which indicates that there is no minimum.

min-lowercase-chars — is the minimum number of lowercase characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

min-numeric-chars — is the minimum number of numeric characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

min-special-chars — is the minimum number of special characters (!@#$%^*()) that passwords must contain. The default value is 0 which indicates that there is no minimum.

min-uppercase-chars — ts the minimum number of uppercase characters that passwords must contain. The default value is 0 which indicates that there is no minimum.

—end—

Example

This example resets these password attributes:

- minimum number of numeric characters that must be used (reset to no minimum)
- minimum number of special characters that must be used (reset to no minimum)

```
user password-policy unset min-numeric-chars min-special-
chars
```

Procedure 8-8
Displaying the current user password policy settings

Display the current user password policy settings.

Step	Action
1	Display the current user password policy settings: `user password-policy show`

—end—

Example

This example displays the current user password policy, which is displayed in the form of a table:

```
+---------- USER PASSWORD POLICY SETTINGS -----------+
| Setting                               | Value      |
+---------------------------------------+------------+
| Minimum Length                        | 8          |
| Minimum Number Lowercase Letters      | 1          |
| Minimum Number Uppercase Letters      | 1          |
| Minimum Number Numeric Chars          | 1          |
| Minimum Number Special Chars          | 1          |
| Minimum Number Changed Chars          | 5          |
| Maximum Run Repeated Chars (0=ignore) | 2          |
| Disallow Dictionary Words             | Off        |
| Disallow User Name                    | Off        |
+---------------------------------------+------------+
```

Procedure 8-9
Enabling SNMP password policy modification capability

Enable the ability to configure the password policy via SNMP.

Step	Action
1	Display the SNMP view tree V12cView: `snmp show viewtree`
2	If the wwpLeosUserMIB sub-tree is displayed, delete it from the view tree. This removes the sub-tree exclusion and enables access to password policy through SNMP: `snmp delete viewtree V12cView sub-tree wwpLeosUserMIB`
3	Display the SNMP view tree to verify that the sub-view has been deleted: `snmp show viewtree`

—end—

Example

Display the SNMP view tree:

```
snmp show viewtree
```

```
+---------------------------------+--------------------------------+--------+
| ViewTreeName                    | SubTree                        | Type   |
+---------------------------------+--------------------------------+--------+
|V12cView                         |iso                             |include |
|V12cView                         |snmpResearch                    |exclude |
|V12cView                         |wwpLeosUserMIB                  |exclude |
+---------------------------------+--------------------------------+--------+
```

The wwpLeosUserMIB sub-tree is excluded. Delete the sub-tree and verify it has been removed from the view tree. snmp delete viewtree V12cView sub-tree wwpLeosUserMIB.

```
snmp show viewtree
```

```
+---------------------------------+--------------------------------+--------+
| ViewTreeName                    | SubTree                        | Type   |
+---------------------------------+--------------------------------+--------+
|V12cView                         |iso                             |include |
|V12cView                         |snmpResearch                    |exclude |
+---------------------------------+--------------------------------+--------+
```

Password policy can now be set through SNMP.

Procedure 8-10
Enabling and disabling user lockout-policy

You must have super user privileges to perform this procedure.

Step	Action
1	Enable or disable user lockout-policy: `user lockout-policy <disable|enable>`

—end—

Procedure 8-11
Configuring the user lockout-policy

You can configure the user lockout-policy. This includes setting the

- fail limit
- lockout time

Note: You must have super user privileges to perform this procedure.

Step Action

To set the user lockout-policy failure limit

1 Configure the user failure limit:

```
user lockout-policy set {fail-limit <NUMBER: 1-5>}
```

where

fail-limit <NUMBER: 1-5>	sets the number of times a user can fail logging in before lockout. Default is 3.

To set the user lockout-policy lockout time

2 Configure the user lockout time:

```
user lockout-policy set lockout-time <duration>
```

where

lockout-time <duration>	sets the amount of time a user is locked out for. Default is 20 minutes.

—end—

Procedure 8-12
Resetting the user lockout-policy

You can reset the failure count and allow a user to log in after a lockout.

> ***Note:*** You must have super user privileges to perform this procedure.

Step	**Action**
1	Reset the user lockout-policy:

```
user lockout-policy reset user <user>
```

where

user <user>	resets the lockout on a user.

—end—

Procedure 8-13
Displaying the user lockout-policy

You can display the user lockout-policy.

> ***Note:*** You must have super user privileges to perform this procedure.

Step	Action
1	Display the user lockout-policy: `user lockout-policy show`

—end—

Example

This example shows the output from the user lockout-policy show command.

```
user lockout-policy show

+-- USER LOCKOUT SETTINGS --+
| Parameter    | Value      |
+--------------+------------+
| Admin State  |    enabled |
| Fail Limit   |          3 |
| Lockout Time |        30m |
+-----------+---------------+

+-------------------------------- USER LOCKOUT TABLE ----------------------------+-----------+
| Username                         | Unlock At              | Last Failure          | Time Left |
+----------------------------------+----------------------+----------------------+-----------+
|              No locked out users |                      |                      |        0s |
+----------------------------------+----------------------+----------------------+-----------+
```

User and user access security

This section explains how to configure authentication methods of devices running SAOS.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server system used to secure networks against unauthorized remote access such as with Telnet. When authenticating a Telnet user, the device sends authentication requests to one or more RADIUS servers. The RADIUS server keeps 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.

39XX/51XX switches support both IPv4 and IPv6 RADIUS servers.

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 three lists of servers: one for user login, one for 802.1x authentication and one for 802.1x accounting.

> ***Note:*** To configure RADIUS, you need to install the Advanced Security license key. To obtain the Advanced Security license key, contact Ciena Sales.

RADIUS servers allow the network operator to configure and control user accounts in one central location instead of having to configure accounts on every device on the network. RADIUS enables access and authentication control to be very flexible in the way it regulates access.

Terminal Access Controller Access-Control System (TACACS) and RADIUS allow user names of up to 32 characters and passwords of up to 128 characters. Local accounts allow 16 characters for user names and passwords.

RADIUS User Login can be enabled or disabled on a global or server-by-server basis. By default, RADIUS is globally enabled. When a RADIUS server is configured on the device, that server is enabled by default.

This table describes the RADIUS servers and what they support.

Table 9-1
RADIUS servers

RADIUS Servers	Supports
RADIUS User Login	• Individual server enable/disable • Configurable UDP port (default is 1812) • Authentication Key, enter clear text or encrypted format
RADIUS User Login accounting	• Individual server enable/disable • Configurable UDP port (default is 1813) • Authentication Key, enter clear text or encrypted format
RADIUX Dot1X Authentication	• Individual server enable/disable • Configurable UDP port (default is 1812) • Authentication Key, enter clear text or encrypted format • Search mode priority or load balance
RADIUS Dot1X Accounting	• Individual server enable/disable • Configurable UDP port (default is 1813) • Authentication Key, enter clear text or encrypted format • Search mode priority or load-balance

A specific priority that controls the order in which servers are contacted can be set for each server, if desired. The server priority continues sequentially and increases or decreases automatically so there are no gaps in server priority. If a new server is added without specifying a priority, it is assigned a priority based on the last server present in the list.

802.1x also uses a RADIUS server to record session statistics. The authenticated port's accounting information is sent to the designated RADIUS server through accounting requests. 802.1x accounting has its own list of servers which can be the same or completely different from the 802.1x RADIUS authentication servers.

RADIUS supports load balancing for 802.1x authentication and 802.1x accounting to determine which server to select for the first attempt to do authentication. Accounting and authorization is tracked separately and globally across ports and sessions. In the load-balanced search mode, 802.1x authentication or 802.1x accounting send authentication or accounting requests to the list of servers in a round robin order. User Login and 802.1x also uses RADIUS servers to record session statistics. The authenticated user or port's accounting information is sent to the designed RADIUS server through accounting requests. User Login accounting and 802.1x accounting have their own lists of servers which can be the same or completely different from the User Login and 802.1x RADIUS authentication servers.

Multi-factor authentication

Multi factor typically means using at least two different kinds of authentication, usually classified as:

- Something you know (such as a password)
- Something you have (such as private key or authenticator device)
- Something you are (biometric)

RADIUS provides mechanisms to request additional information from the user. SAOS works with any text-based multi-factor authentication provided by the RADIUS server, such as RSA authenticators or the Google Authenticator application.

RADIUS servers can reply to requests with an Access-Challenge response. This message can carry a Reply-Message attribute containing an arbitrary prompt. SAOS responds to these by displaying the prompt if provided or by supplying a default prompt, reading a string back from the user and sending that response back to the server in a Challenge-Response message.

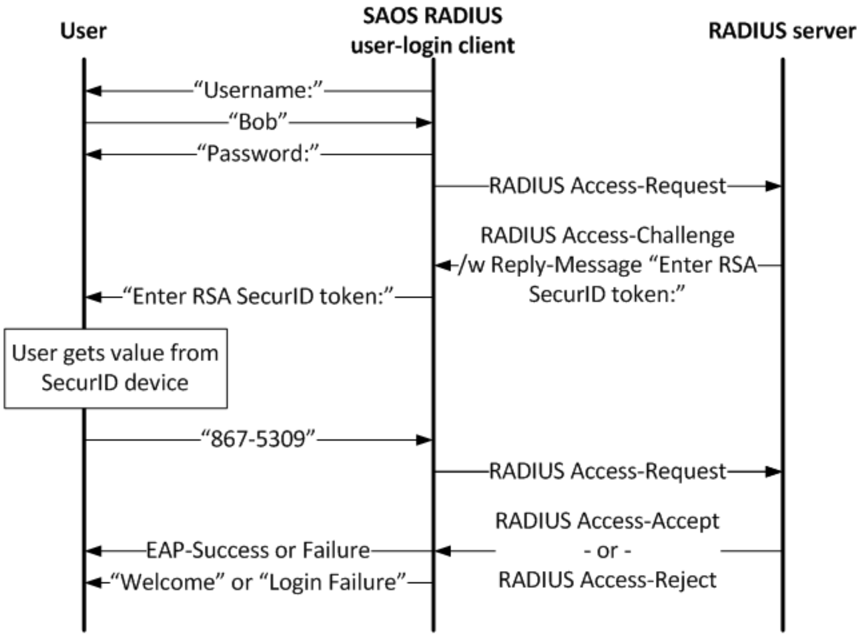
This allows the server to perform an arbitrary number of exchanges with the user which can include challenge response, requesting a value from the authenticator, requesting a new password or asking a question such as what was your mother's maiden name.

TACACS+ provides a similar mechanism. A TACACS+ server can reply to access requests with a REPLY that contains a TAC_PLUS_AUTHEN_STATUS_GETDATA indicating that it needs data other than the username or password. This reply may include a server_msg which can be used as a prompt.

Any information entered by the user can be sent back as a user_msg in a CONTINUE packet.

This figure shows a multi-factor authentication sequence example.

Figure 9-1
Multi-factor authentication sequence example


User
SAOS RADIUS user-login client
RADIUS server
"Username:"
"Bob"
"Password:"
RADIUS Access-Request
RADIUS Access-Challenge /w Reply-Message "Enter RSA SecurID token:"
"Enter RSA SecurID token:"
User gets value from SecurID device
"867-5309"
RADIUS Access-Request
RADIUS Access-Accept - or - RADIUS Access-Reject
EAP-Success or Failure
"Welcome" or "Login Failure"

RADIUS and TACACS+ configuration

For RADIUS and TACACS+ multi factor, the authentication process is mainly controlled by the server. The client (SAOS) is only required to properly show server prompts to the user and present the user's responses to the server. Little configuration is required. The only exception to this is to control how TACACS+ collects the password. SAOS's TACACS+ client prompts for the username and password before contacting the server.

In multi-factor authentication, the client prompts for the username, and then lets the server direct all additional prompts. This is enabled with the command: `tacacs authentication set enhanced multi-factor <on|off>`.

> ***Note:*** A notification/trap is generated if the authentication fails because the client is unable to reach the TACACS server.

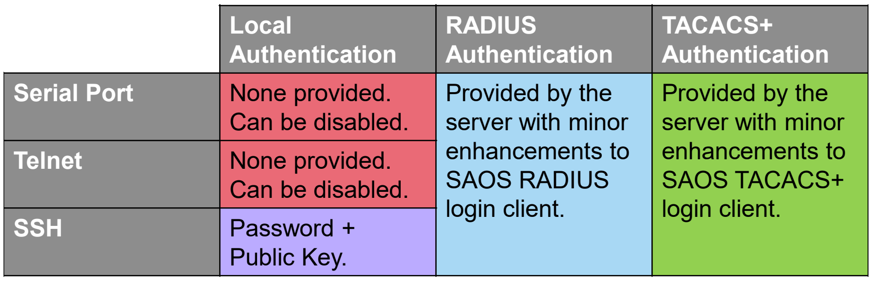
SSH multi-factor authentication

Local multi-factor authentication can be done using SSH. Prior to SAOS 6.14, the SSH server supported logon with either a password or public key authentication. In SAOS 6.14 or later, SSH can be configured to require both a password and a public key to provide a valid form of multi-factor authentication through the command: `ssh server set multi-factor-auth <on|off>`.

> ***Note:*** The SSH multi-factor authentication setting is only applied to user accounts that have public keys installed. This prevents accidental lockout since public keys are not part of the configuration file.

This figure describes the coverage for multi-factor authentication.

Figure 9-2
Multi-factor authentication coverage



	Local Authentication	RADIUS Authentication	TACACS+ Authentication
Serial Port	None provided. Can be disabled.	Provided by the server with minor enhancements to SAOS RADIUS login client.	Provided by the server with minor enhancements to SAOS TACACS+ login client.
Telnet	None provided. Can be disabled.		
SSH	Password + Public Key.		

RADIUS Vendor-Specific Attributes (VSA)

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access device and the RADIUS server, by using the vendor-specific attribute, attribute 26. Attribute 26 allows vendors to support their own extended attributes otherwise not suitable for general use.

The Ciena RADIUS client supports vendor-specific options or user login which can be used to define the user privilege level assigned to the user being authenticated.

This table describes the VSA attributes.

Table 9-2
VSA attributes

VSA Attributes	Description
VSA for new installations and Packet Networking devices that interwork with the 4200 platform.	• attribute type: 26 (VSA) • vendor: 1271 (ciena) • vsa-sub-type: 10 • integer to indicate privilege level: — 1 (limited) — 2 (admin) — 3 (super-user) — 4 (diag)
Ciena also supports a legacy VSA.	• attribute type: 26 9VSA) • vendor: 1271 (ciena) • vsa-sub-type: 1 and one of the following numbers to indicate user privilege level: — 1 (limited) — 2 (admin) — 3 (super-user) — 4 (diag)

> ***Note:*** Switches that run older software require the legacy VSA. You can configure servers that provide authentication to switches running older software with the legacy VSA or both VSAs.

RADIUS procedures are:

- "Configuring RADIUS" on page 9-12
- "Enabling and disabling RADIUS accounting" on page 9-17
- "Displaying RADIUS statistics" on page 9-18
- "Clearing RADIUS statistics" on page 9-21

Secure RADIUS (TLS Transport)

RFC 6614 defines Transport Layer Security (TLS) Transport mapping for RADIUS, which provides a secure connection for the transport of RADIUS messages. SAOS implements secure Radius for user login and accounting.

Secure RADIUS is modeled as a manager, client, and authentication source completely independent of UDP RADIUS, although most non-transport-related settings and behaviors are identical.

To use Secure RADIUS, the SAOS switch client and external server must be configured with signed device certificates and private keys. They are usually preconfigured with the CA certificate (chain) that signed each other's device certificates. The server hostname or IP is used to add a Secure RADIUS server on SAOS.

To perform Secure RADIUS AAA, the SAOS switch initiates a TLS connection to the server. The two endpoints perform configured authentications and establish a TLS connection. RADIUS messages are then transmitted by means of the TLS connection.

RFC 6614 includes a number of mechanisms for TLS authentication and authorization that the SAOS switch supports:

- Certificate path validation, that is, checking certificate fields against trusted CA/CRLs
- End-entity certificate based authorization, that is, fingerprint checking
- Subject Name Authorization, that is, checking certificate fields against locally configured peer DNS name or IP address

  Note: Secure RADIUS (TLS) is enabled by default. No default servers are configured and a license is required to use it.

Secure RADIUS procedures are:

- “Creating and installing device certificates” on page 9-23
- “Configuring Secure Radius” on page 9-25
- “Configuring Secure RADIUS accounting servers” on page 9-28
- “Displaying Secure RADIUS certificates” on page 9-29
- “Displaying Secure RADIUS OCSP responders” on page 9-30
- “Displaying Secure RADIUS information” on page 9-31
- “Displaying Secure RADIUS user statistics” on page 9-33
- “Clearing Secure RADIUS statistics” on page 9-35

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) provides an industry standard security protocol for controlling AAA functions. It also provides security by using a shared key to encrypt information between the NAS and the authentication server.

> ***Note:*** To enable TACACS+ commands, the Security feature license must be installed with the software license install command. If you upgrade from a previous software release without first installing the Security feature license, TACACS is disabled and its configuration is not supported.

TACACS+ performs the following AAA 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 have access to a device. Authorization is performed only if authentication was done by TACACS+.

  Note 1: When authorization is enabled, the switch authorizes every user command with a RADIUS or TACACS server before execution. In order for this to operate correctly, a server must be correctly configured to allow or deny commands for each user or group of users.

  Servers deny access by default, allowing only the commands specifically configured as allowed. If you enable authorization on the switch without any server configuration, every command is denied and you are unable to execute any commands on the switch.

  Note 2: The user group of which an account is a member, that is, super, admin, or limited, already provides some degree of command authorization.

  Note 3: A notification/trap is generated if the authentication fails because the client is unable to reach the TACACS server.

  For a general explanation of how commands are authorized by user group, see "User groups" on page 2-1.

  For information about how the different user groups are authorized to use those commands, see the "Access" column for all commands in *39XX/51XX Switches and Platforms Command Reference*.
- Accounting- Records user actions to perform security audits or for billing purposes. Accounting is be performed only if authentication was done by TACACS+.

  Note: If you use only authorization, the server still logs login attempts so there is some "accounting" by default.

  This is also true if you use authentication and authorization, where the server typically logs shell login attempts and command authorization attempts.

The TACACS+ protocol client is supported where the device operates as a NAS. The TACACS+ client support up to 8 authentication, authorization and accounting servers by means of the CLI or SNMP. If a TACACS+ server is not configured, a locally-configured password file is used for authentication. Local authentication is used only if the user authentication provider order is configured properly to allow for it.

Note 1: TACACS+ is not compatible with previous TACACS and XTACACS protocols.

Note 2: To enable TACACS commands, the Security feature license must be installed with the `software license install` command. If you upgrade from a previous software release without first installing the Security feature license, TACACS is disabled and its configuration is not supported.

TACACS+ configuration

TACACS+ can be enabled and disabled on a global basis, and can also be enabled on specific Authentication, Authorization or Accounting servers. (Note that authentication must be enabled for Authorization or Accounting to be operational.)

By default TACACS+ is globally enabled, only Authentication is enabled, and no default TACACS+ servers are configured. Up to 8 servers can be configured for each of the individual AAA functions and the global lists. If the authentication, authorization, or accounting server list cannot be used or has no specified servers, the global list is used by default. The global list is also used if no TACACS+ authentication, authorization or accounting servers are specified. In addition, the servers can be searched by their priority or cached value (last accessed).

Each TACACS+ server has a unique priority number in the specific AAA/or global list between 1 and 8, where 1 is the highest priority. The server priority continues sequentially and increases or decreases automatically so there are no gaps in server priority. If a new server is added without specifying a priority, it is assigned a priority based on the last server present in the list. In addition to priority, the TCP port number can be specified for each server. If it is not specified, the default port number is 49.

When performing authentication, the login password allows all ASCII values from 32 to 126.

TACACS authentication fails under these circumstances:

- The TACACS server operational state is DISABLED.
- The number of authentication retries has been met.
- If the `user auth set method` command is not used to configure TACACS as the authentication method.
- If the `tacacs set key` command has not been configured (or was entered incorrectly).
- If the client is unable to reach the TACACS server. In this case, a notification/trap is generated.

If all servers have been tried without success, or if a server rejects the user credentials, then the authentication is considered to have failed. The user login/authentication attempt is denied.

After a user is successfully authenticated, the privilege level is derived from the privilege level retrieved from the TACACS Server by mapping the server numerical levels to four user group categories on a Ciena TACACS client, as shown in Table 9-3. Authenticated users can execute commands and their associated arguments, and these are passed as fully expanded CLI commands to the TACACS+ server. Attribute-Value types other than "cmd" and "cmd-arg" are not supported.

The TACACS+ server must be configured with the correct TACACS Privilege Level for each account.

This table provides the mapping of TACACS to CLI user privilege levels.

Table 9-3
TACACS to Default CLI User Privilege Levels

TACACS Privilege	TACACS Privilege Level	CLI Privilege Level
Read-Write-Create	10-14	super
Read-Write	2-9	admin
Read	0-1	limited user
Unrestricted	15	diag

When session and command accounting are enabled, start and stop messages are sent for each login session and command that is executed. TACACS+ statistics can be viewed and cleared.

TACACS+ procedures are:

- “Configuring TACACS+ authentication” on page 9-36
- “Configuring TACACS+ authorization” on page 9-38
- “Configuring TACACS+” on page 9-41

User accounting settings for external accounting

This table describes the user settings for external user accounting.

Table 9-4
User accounting settings

User account setting	Authentication method	Description
Default	RADIUS	RADIUS is used for user accounting, if configured.
	TACACS+	TACACS+ is used for user accounting, if configured.
	Local	No external user accounting is done.
RADIUS	RADIUS, TACACS+ or Local	RADIUS is used for user accounting, regardless of how the user was authenticated. This setting is applied when a user session starts. It does not change existing sessions.
TACACS	TACACS+, RADIUS or Local	TACACS+ is used for user accounting, regardless of how the user was authenticated. This setting is applied when a user session starts. It does not change existing sessions.

User accounting procedures are:

- “Configuring TACACS+ and RADIUS user accounting” on page 9-43
- “Displaying TACACS+ and RADIUS user accounting” on page 9-44

Authentication

Authentication procedures are:

- “Configuring authentication providers” on page 9-45
- “Displaying authentication providers and statistics” on page 9-47
- “Clearing authentication statistics” on page 9-48
- “Removing authentication methods” on page 9-49

Procedure 9-1
Configuring RADIUS

You can log in to a RADIUS server, and then set the global parameters for using RADIUS authentication. SAOS software supports RADIUS over IPv6.

You can individually configure 802.1x authentication and 802.1x accounting servers to query RADIUS servers in either priority or load balancing order. For user login accounting, the configured RADIUS servers can query off of the last accessed server.

> ***Note 1:*** RADIUS attributes are set globally, that is, they apply to all RADIUS servers.
>
> ***Note 2:*** The default values have been set to enable proper operation, for example, successful RADIUS authentication of dot1x sessions.Ensure that you have a good understanding of timeout values before changing the timeout value defaults.
>
> ***Note 3:*** The value of an 802.1x authenticator server-timeout must be greater than (radius dot1x-auth timeout * (radius dot1x-auth retries +1)). A shorter authenticator server-timeout prevents the RADIUS client from detecting and gray-listing unresponsive RADIUS servers that can prevent authentication from completing successfully. Ideally, the authentication server-timeout must be greater than (radius dot1x-auth timeout * (radius dot1x-auth retries +1)) * (number of enabled radius dot 1x-auth servers), particularly in priority search-mode.

Step **Action**

1 Enable RADIUS globally for RADIUS login and dot1x, authentication and accounting:

```
radius enable
```

2 Add the RADIUS servers and server attributes for login and dot1x, authentication and accounting:

```
radius user-login add server <IP address or host
name[1..63]> priority <NUMBER: 1..8> udp-port <NUMBER:
1..65535>
radius user-acct add server <IP address or host
name[1..63]> priority <NUMBER: 1..8> udp-port <NUMBER:
1..65535>
radius dot1x-auth add server <IP address or host
name[1..63]> priority <NUMBER: 1..8> udp-port <NUMBER:
1..65535>
```

```
radius dot1x-acct add server <IP address or host
name[1..63]> priority <NUMBER: 1..8> udp-port <NUMBER:
1..65535>
```

where

server <IP address or host name[1..63]>	is the IP address or hostname for login or dot1x, authentication or accounting.
priority <NUMBER: 1..8>	is the priority of the server.
udp-port <NUMBER: 1..65535>	is the UDP port of RADIUS server.

3 (Optional) Set the attributes of RADIUS server access.

```
radius user-login set key <Password String> retries
<NUMBER: 0..3> timeout <SECONDS: 1..3> search-method
<cached | priority>

radius user-login set service-type <on | off>

radius user-acct set key <Password String> retries
<NUMBER: 0..3> timeout <SECONDS: 1..3> search-method
<cached | priority>

radius dot1x-auth set greylist-timeout <duration:
[N[yMwdhms]* e.g. 1h10m3s> key <Password String> retries
<NUMBER: 0..3> timeout <SECONDS: 1..3> config-reauth
<on|off> search-method <balanced | priority>

radius dot1x-acct set greylist-timeout <duration:
[N[yMwdhms]* e.g. 1h10m3s> key <Password String> retries
<NUMBER: 0..3> timeout <SECONDS: 1..3> search-method
<balanced | priority>
```

where

key <Password String>	is the RADIUS key.
retries <NUMBER: 0..3>	is the maximum retries.
timeout <SECONDS: 1..3>	is the response time from RADIUS server.
greylist-timeout <duration: [N[yMwdhms]* e.g. 1h10m3s>	sets the greylist timeout duration: 1 minute to 4 hours.

where

config-reauth <on|off>	enables or disables RADIUS 802.1x configuration reauthorization. When config-reauth is on, the RADIUS 802.1x authorization settings are changed immediately causing re-authentication of all currently authenticated ports. When config-reauth is off, any changes to those settings do not cause immediate re-authentication, but are used on the next authentication attempt.
search-method <cached | priority>	is used to set the search method for RADIUS user-login. and accounting. Load balancing is used to determine which server is selected for the first attempt to do authentication or accounting on a per-port, per-session basis.
search-method <balanced | priority>	is used to set the search method for RADIUS 802.1x authentication and 802.1x accounting. Load balancing is used to determine which server is selected for the first attempt to do authentication or accounting on a per-port, per-session basis.
service-type <on | off>	specifies whether there will be a "Service-Type" field in the Access_Request packet sent to the RADIUS server. The value “on” specifies that the “Service-Type” field will be present in the Access_Request packet. The value “off” specifies that the “Service-Type” field will not be present in the Access_Request packet. ***Note:*** If the RADIUS server assigns limited access privilege level to all users, specify “service-type off”.

4 (Optional) Verify RADIUS configurations and check the RADIUS server statistics.

```
radius show [statistics]
```

where these attributes are available	
statistics	displays only RADIUS statistics.

—end—

Example

This example shows sample output for the radius show command.

```
> radius show
+--------------------------- RADIUS ATTRIBUTES ---------------------------+
| Parameter                                            |      Value       |
+------------------------------------------------------+------------------+
| Radius Admin State                                   | Enabled          |
| Radius Oper State                                    | Enabled          |
+------------------------------------------------------+------------------+
| User Login Retries                                   | 3                |
| User Login Timeout                                   | 1                |
| User Login Search Method                             | Priority         |
| User Login Key                                       |                  |
+------------------------------------------------------+------------------+
| User Login Accounting Admin State                    | Disabled         |
| User Login Accounting Retries                        | 3                |
| User Login Accounting Timeout                        | 1                |
| User Login Accounting Search Method                  | Priority         |
| User Login Accounting Key                            |                  |
+------------------------------------------------------+------------------+
| 802.1x Authentication Retries                        | 3                |
| 802.1x Authentication Timeout                        | 1                |
| 802.1x Authentication Search Method                  | Priority         |
| 802.1x Authentication Greylist Timeout               | 600              |
| 802.1x Authentication Configuration Reauthorization  | Off              |
| 802.1x Authentication Key                            |                  |
+------------------------------------------------------+------------------+
| 802.1x Accounting Admin State                        | Disabled         |
| 802.1x Accounting Retries                            | 3                |
| 802.1x Accounting Timeout                            | 1                |
| 802.1x Accounting Search Method                      | Priority         |
| 802.1x Accounting Greylist Timeout                   | 600              |
| 802.1x Accounting Interval                           | 86400            |
| 802.1x Accounting Key                                |                  |
+------------------------------------------------------+------------------+

+------------------------------------------ RADIUS USER LOGIN SERVER TABLE ----------------------+
| IP Address                         |HostName                          |Pri|UDP  |State   |Used |
|                                    |                                  |   |Port |Adm|Oper|Last |
+------------------------------------+----------------------------------+---+-----+--------+-----+
| 2001:db8:f018:1:202:5aff:fe01:b449 |2001:db8:f018:1:202:5aff:fe01:b449|1  |1812 |Ena|Ena |x    |
+------------------------------------+----------------------------------+---+-----+--------+-----+

+--------------------------------RADIUS USER LOGIN ACCOUNTING SERVER TABLE ----------------------+
| IP Address                         |HostName                          |Pri|UDP  |State   |Used |
|                                    |                                  |   |Port |Adm|Oper|Last |
+------------------------------------+----------------------------------+---+-----+--------+-----+
| 2001:db8:f018:1:202:5aff:fe01:b449a|2001:db8:f018:1:202:5aff:fe01:b44a|1  |1813 |Ena|Ena |x    |
+------------------------------------+----------------------------------+---+-----+--------+-----+

+--------------------------------RADIUS 802.1X AUTHENTICATION SERVER TABLE --------------------------+
| IP Address                         |HostName                          |Pri|UDP  |State   |Greylist |
|                                    |                                  |   |Port |Adm|Oper|Remaining|
+------------------------------------+----------------------------------+---+-----+--------+---------+
| 2001:0db8:f018:aaaa::aaaa          |v6server                          |1  |1812 |Ena|Dis |53       |
| 2001:0db8:f018:aaaa::bbbb          |v6server2                         |2  |1812 |Ena|Ena |0        |
| 2001:0db8:f018:aaaa::cccc          |v6server3                         |3  |1812 |Ena|Ena |0        |
| Unresolved                         |v6server4                         |4  |1812 |Ena|Dis |0        |
+------------------------------------+----------------------------------+---+-----+--------+---------+

+--------------------------------RADIUS 802.1X ACCOUNTING SERVER TABLE ------------------------------+
| IP Address                         |HostName                          |Pri|UDP  |State   |Greylist |
|                                    |                                  |   |Port |Adm|Oper|Remaining|
+------------------------------------+----------------------------------+---+-----+--------+---------+
| 2001:0db8:f018:aaaa::aaaa          |v6server                          |1  |1813 |Ena|Dis |58       |
| 2001:0db8:f018:aaaa::bbbb                      |v6server2                                    |2   |1813   |Ena|Ena    |0           |
| 2001:0db8:f018:aaaa::cccc                      |v6server3                                    |3   |1813   |Ena|Ena    |0           |
| Unresolved                                     |v6server4                                    |4   |1813   |Ena|Dis    |0           |
+------------------------------------------------+---------------------------------------------+----+-------+-----------+------------+
```

```
> radius show statistics
+------------------------------- RADIUS SERVER 1 STATISTICS -------------------------------+
| Server IP Address         | 2001:0db8:f018:aaaa::aaaa                                    |
| HostName                  | v6server                                                     |
|                           | 2001:0db8:f018:aaaa::aaaa                                    |
+---------------------------+---------------+---------------+---------------+---------------+
|                           | User Login    | User Acct     | Dot1x Auth    | Dot1x Acct    |
+---------------------------+---------------+---------------+---------------+---------------+
| Requests                  | 0             | 0             | 8             | 8             |
| Access Accepts            | 0             | 0             | 8             | 0             |
| Access Challenges         | 0             | 0             | 8             | 0             |
| Access Rejects            | 0             | 0             | 0             | 0             |
| Accounting Responses      | 0             | 0             | 0             | 16            |
| Retransmission            | 0             | 0             | 0             | 0             |
| Bad Authenticators        | 0             | 0             | 0             | 0             |
| Timeouts                  | 0             | 0             | 0             | 0             |
| Unknown Types             | 0             | 0             | 0             | 0             |
| Packets Dropped           | 0             | 0             | 8             | 8             |
| Malformed Rx Responses    | 0             | 0             | 0             | 0             |
| Round Trip Time (sec)     | 0.00          | 0.00          | 0.00          | 0.00          |
+---------------------------+---------------+---------------+---------------+---------------+
```

Note: If the RADIUS server does not respond to requests or is not accessible, the only way to access the device is through SNMP/EMS unless you have configured the authorization provider to use the local database as a second priority authorization method.

This example shows the de-activation of the Access_Request packet sent to the RADIUS server.

```
radius user-login set service-type off

radius user-login show

+------------------------- RADIUS ATTRIBUTES -------------------------+
| Parameter                                  | Value                  |
+--------------------------------------------+------------------------+
| Radius Admin State                         | Enabled                |
| Radius Oper State                          | Enabled                |
| Preferred Source Address                   | default                |
| Preferred Source IP                        |                        |
+---------------------------------------------------------------------+
| User Login Retries                         | 3                      |
| User Login Timeout                         | 1                      |
| User Login Search Method                   | Priority               |
| User Login Key                             |                        |
| User Login service-type attribute          | off                    |
+--------------------------------------------+------------------------+
```

Procedure 9-2
Enabling and disabling RADIUS accounting

You can

- enable or disable RADIUS 802.1x accounting
- enable or disable RADIUS user login accounting

Step **Action**

To enable or disable RADIUS 802.1x accounting

1 Enable RADIUS 802.1x accounting:

```
radius dot1x-acct <enable|disable>
```

To enable or disable RADIUS user login accounting

2 Enable RADIUS user login accounting:

```
radius user-acct <enable|disable>
```

—end—

Procedure 9-3
Displaying RADIUS statistics

You can display RADIUS

- user login statistics
- user login server statistics
- user login accounting statistics
- user login accounting server statistics
- 802.1x authentication statistics
- 802.1x authentication server statistics
- 802.1x accounting statistics
- 802.1x accounting server statistics

Step **Action**

To display RADIUS user login statistics

1 Display RADIUS user login statistics:

```
radius user-login show {statistics}
```

where

statistics	displays RADIUS user login statistics.

To display RADIUS user login server statistics

2 Display RADIUS user login server statistics:

```
radius user-login show server <server> {statistics}
```

where

server <server>	is the RADIUS server IP address or host name.
statistics	displays RADIUS user login statistics.

To display user RADIUS user accounting statistics

3 Display RADIUS user login accounting statistics:

```
radius user-acct show {statistics}
```

where

statistics	displays RADIUS user login accounting statistics.

To display user RADIUS user accounting server statistics

4 Display RADIUS user login server statistics:

```
radius user-acct show server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics displays RADIUS user login accounting statistics.

To display user RADIUS 802.1x authentication statistics

5 Display RADIUS 802.1x authentication statistics:

```
radius dot1x-auth show {statistics}
```

where

statistics clears RADIUS 802.1x authentication statistics.

To display user RADIUS 802.1x authentication server statistics

6 Display RADIUS 802.1x authentication server statistics:

```
radius dot1x-auth show server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics displays RADIUS 802.1x authentication statistics.

To display user RADIUS 802.1x accounting statistics

7 Display RADIUS 802.1x authentication statistics:

```
radius dot1x-acct show {statistics}
```

where

statistics displays RADIUS 802.1x accounting statistics.

To display user RADIUS 802.1x accounting server statistics

8 Display RADIUS 802.1x authentication server statistics:

```
radius dot1x-acct show server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics display RADIUS 802.1x accounting statistics.

—end—

Example

This example shows sample output for the radius dot1x-auth show server <server> statistics command.

```
> radius dot1x-auth show server 10.25.35.46 statistics
```

```
+---------------------- DOT1X AUTHENTICATOR PORT 3 RADIUS STATISTICS ----------------------+
|Statistic                |                             Value                              |
+-------------------------+----------------------------------------------------------------+
|Requests                 |308                                                             |
|Access Accepts           |79                                                              |
|Access Challenges        |79                                                              |
|Access Rejects           |0                                                               |
|Retransmissions          |357                                                             |
|Bad Authenticators       |0                                                               |
|Timeouts                 |469                                                             |
|Unknown Types            |0                                                               |
|Packets Dropped          |0                                                               |
+-------------------------+----------------------------------------------------------------+
|Last Server:             |                                                                |
|   IP Address            |10.25.35.46                                                     |
|   Hostname              |10.25.35.46                                                     |
|   Last Event            |Access Accept                                                   |
+-------------------------+----------------------------------------------------------------+
```

Procedure 9-4
Clearing RADIUS statistics

You can clear RADIUS

- user login statistics
- user login server statistics
- user login accounting statistics
- user login accounting server statistics
- 802.1x authentication statistics
- 802.1x authentication server statistics
- 802.1x accounting statistics
- 802.1x accounting server statistics

Step Action

To clear RADIUS user login statistics

1 Clear RADIUS user login statistics:

```
radius user-login clear {statistics}
```

where

statistics	clears RADIUS user login statistics.

To clear RADIUS user login server statistics

2 Clear RADIUS user login server statistics:

```
radius user-login clear server <server> {statistics}
```

where

server <server>	is the RADIUS server IP address or host name.
statistics	clears RADIUS user login statistics.

To clear user RADIUS user accounting statistics

3 Clear RADIUS user login accounting statistics:

```
radius user-acct clear {statistics}
```

where

statistics	clears RADIUS user login accounting statistics.

To clear user RADIUS user accounting server statistics

4 Clear RADIUS user login server statistics:

```
radius user-acct clear server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics clears RADIUS user login accounting statistics.

To clear user RADIUS 802.1x authentication statistics

5 Clear RADIUS 802.1x authentication statistics:

```
radius dot1x-auth clear {statistics}
```

where

statistics clears RADIUS 802.1x authentication statistics.

To clear user RADIUS 802.1x authentication server statistics

6 Clear RADIUS 802.1x authentication server statistics:

```
radius dot1x-auth clear server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics clears RADIUS 802.1x authentication statistics.

To clear user RADIUS 802.1x accounting statistics

7 Clear RADIUS 802.1x authentication statistics:

```
radius dot1x-acct clear {statistics}
```

where

statistics clears RADIUS 802.1x accounting statistics.

To clear user RADIUS 802.1x accounting server statistics

8 Clear RADIUS 802.1x authentication server statistics:

```
radius dot1x-acct clear server <server> {statistics}
```

where

server <server> is the RADIUS server IP address or host name.

statistics clears RADIUS 802.1x accounting statistics.

—end—

Procedure 9-5
Creating and installing device certificates

Create and install a device certificate for use by RadSec, Syslog TLS, or 802.1x.

Prerequisite

Access to a certificate authority or OpenSSL to sign the X.509 certificate.

Step **Action**

1 At an external xFTP server, create a configuration file with the subject name for the device certificate.

2 At the SAOS switch, create a private key, download the certificate configuration file from the xFTP server, and generate a certificate signing request (CSR) using the following command. The CSR is then uploaded to the ftp server as <filename>.csr

```
system security pkix certificates csr generate cert-name
<name> key-type <key-type> ftp-server <IP address or host
name> filename <String[1..127]>
```

3 At a Certificate Authority or using tools like OpenSSL, sign the certificate.

4 Copy the signed certificate to the FTP server.

5 At the SAOS switch, install the certificate:

```
system security pkix certificates install cert-name
<cert-name> cert-only ftp-server <IP address or host
name> filename <String[1..127]>
```

6 Verify the key and certificate.

```
system security pkix certificates show
```

Example

This example shows how to configure device certificates.

```
Configuration guide file:
[ req ]
distinguished_name = req_distinguished_name
prompt = no
[ req_distinguished_name ]
C = US
ST = Maryland
L = Hanover
O = YourCompany
OU = YourDepartment
CN = SaosCertificate
emailAddress = SaosTest@none.invalid
```

```
> system security pkix certificates csr generate cert-name test key-type 
rsa2048 ftp-server 10.10.10.10 filename radsec.cnf login-id bob echoless-
password
Enter Password:
Generating RSA private key, 2048 bit long modulus ................+++
.....................................................+++
> system security pkix certificates install cert-name test cert-only ftp-
server 10.10.10.10 filename radsec.pem loginid bob echoless-password
> system security pkix certificates show

+--------------------- DEVICE CERTIFICATE ----------------------+
| Parameter            | Value                                   |
+----------------------+-----------------------------------------+
| Certificate Name     | test                                    |
+----------------------+-----------------------------------------+
| Private Key          | Present                                 |
| Key Type             | RSA (2048)                              |
+----------------------+-----------------------------------------+
| Device Certificate   |                                         |
|  Subject Common Name | SaosCertificate                         |
|  Issuer Common Name  | MyCA                                    |
|  Valid To            | Oct  5 15:02:01 2018 GMT (11 months)    |
+----------------------+-----------------------------------------+
```

Procedure 9-6
Configuring Secure Radius

Configure Secure RADIUS (RadSec) to establish a secure connection for the transport of RADIUS messages.

Step	Action

1 Install a device certificate (see "Creating and installing device certificates" on page 9-23).

2 Configure radsec to use that certificate, giving it the cert-name used when creating/installing the device certificate:

```
radsec set cert-name <cert-name>
```

3 Verify the radsec certificate:

```
radsec show certificate
```

4 Add a server:

```
radsec user-login add server <IP address or host name>
```

5 Use the following command to optionally configure Secure Radius to check the configured server's hostname or IP address against the Subject Common Name or Subject Alternative Name fields in the server's certificate:

```
radsec set check-ip-host on|off
```

6 Use this command to optionally enable or disable ciphersuites:

```
radsec algorithm cipher-suite enable | disable cipher-
suite <String>
```

Configure Secure Radius OCSP client

OCSP can optionally be enabled to do real time certificate status checks when validating a Secure Radius server's X.509 certificate.

7 Enable or disable OCSP checking:

```
radsec ocsp enable | disable
```

8 Set optional default OCSP responder.

```
radsec ocsp set default-responder <String[1..255]>
```

9 Configure user authentication to use secure radius, then local authentication if it can't communicate with the secure radius server.

```
user auth set order local | radius | secrad | tacacs
```

Display current RadSec configuration

10 Display RadSec configuration:

```
radsec user-acct show
```

Display RadSec statistics

11 Display RadSec statistics:

```
radsec user-acct show statistics
```

Example

This example configures radsec.

```
> radsec set cert-name test
> radsec show certificate
+------------------ RADSEC DEVICE CERTIFICATE ------------------+
| Parameter            | Value                                  |
+----------------------+----------------------------------------+
| Certificate Name     | test                                   |
+----------------------+----------------------------------------+
| Private Key          | Present                                |
| Key Type             | RSA (2048)                             |
+----------------------+----------------------------------------+
| Device Certificate   |                                        |
|  Subject Common Name | SaosCertificate                        |
|  Issuer Common Name  | MyCA                                   |
|  Valid To            | Oct  5 15:02:01 2018 GMT (11 months)   |
+----------------------+----------------------------------------+

> radsec user-login add server 10.10.10.10
> radsec set check-ip-host on
> radsec algorithm cipher-suite enable cipher-suite
TLS_RSA_WITH_AES_128_CBC_SHA
> radsec algorithm cipher-suite disable cipher-suite TLS_RSA_WITH_RC4_128_MD5
> radsec ocsp set default-responder http://10.1.1.100:8080
> user auth set order radsec,local
> radsec user-acct show
+------------------------- RADSEC ATTRIBUTES --------------------+
| Parameter                         | Value                      |
+-----------------------------------+----------------------------+
| RadSec Admin State                | Disabled                   |
| RadSec Oper State                 | Disabled                   |
+-----------------------------------+----------------------------+
| Timeout                           | 6s                         |
| Search Method                     | Priority                   |
| Minimum TLS Version               | TLSv1.1                    |
| Greylist Timeout                  | 10m                        |
| Device Certificate Name           | test                       |
| Device Certificate/Key            | Ok                         |
| Device Certificate [SHA-1]        | FA:78:91:FC:61:11:1D:F6... |
| Check Peer Certificate            | Enabled                    |
| Check Peer IP/Hostname            | Disabled                   |
| Check Peer Fingerprint            | Enabled                    |
| Check Cert Time Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| User Accounting Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| OCSP                              |                            |
|     Admin State                   | Disabled                   |
|     Responder Preference          | aia                        |
|     Default Responder             |                            |
|     Nonce                         | On                         |
+-----------------------------------+----------------------------+
+------------- RADSEC USER LOGIN ACCOUNTING SERVER TABLE ------------+
| IP Address     | HostName      |Pri|Port | State    |Used|Greylist...|
+---------------+---------------+---+-----+---+-----+----+-----------+
| 10.121.240.170| 10.121.240.170|1  |2083 |Ena|Dis  |    |0          |
+---------------+---------------+---+-----+---+-----+----+-----------+

> radsec user-acct show statistics
+--------------- RADSEC USER ACCT SERVER 1 STATISTICS ---------------+
| Server IP Address      | 10.121.240.170                            |
| Hostname               | 10.121.240.170                            |
+------------------------+-------------------------------------------+
| Connection Attempts    | 4                                         |
| Successful Connections | 3                                         |
| Failed TCP Connections | 0                                         |
| Failed TLS Connections | 1                                         |
| Timed Out Connections  | 0                                         |
| Unexpected Closes      | 0                                         |
| Closed Connections     | 3                                         |
+------------------------+-------------------------------------------+
| Last Transport Error   | Unknown                                   |
+------------------------+-------------------------------------------+
| Radius Requests        | 3                                         |
| Access Accepts         | 0                                         |
| Access Rejects         | 0                                         |
| Access Challenges      | 0                                         |
| Responses              | 3                                         |
| Malformed Responses    | 0                                         |
| Bad Authenticators     | 0                                         |
| Unknown Types          | 0                                         |
| Packets Dropped        | 0                                         |
| Unsupported Extension  | 0                                         |
+------------------------+-------------------------------------------+
```

Procedure 9-7
Configuring Secure RADIUS accounting servers

Adds a host for radsec user-login. Attributes not specified are set to the default value. Host is enabled by default.

You can:

- add a RadSec accounting server
- remove a RadSec accounting server
- enable user accounting
- disable user accounting

Step **Action**

Add and remove RadSec accounting servers

1 Add a RadSec accounting server:

```
radsec user-acct add <Ip Address>
```

2 Remove a RadSec accounting server:

```
radsec user-acct remove <Ip Address>
```

Enable and disable RadSec accounting

3 Enable RadSec accounting:

```
radsec user-acct enable
```

4 Disable RadSec accounting:

```
radsec user-acct disable
```

—end—

Procedure 9-8
Displaying Secure RADIUS certificates

You can display RadSec certificates.

Step **Action**

1 Display RadSec certificates:

```
radsec show certificate
```

—end—

Procedure 9-9
Displaying Secure RADIUS OCSP responders

You can display RadSec OCSP responders.

Step **Action**

1 Display RadSec OCSP responders:

```
radsec ocsp show
```

—end—

Example

This example shows the output from the radsec ocsp show command.

```
radsec ocsp show
+-------------------- RADSEC OCSP ATTRIBUTES ----------------------+
| Parameter            | Value                                     |
+----------------------+-------------------------------------------+
| Admin State          | Disabled                                  |
| Default Responder    |                                           |
| Nonce                | On                                        |
| Responder Preference | aia                                       |
+----------------------+-------------------------------------------+
```

Procedure 9-10
Displaying Secure RADIUS information

You can display Secure RADIUS

- RadSec server statistics
- RadSec attributes

Step Action

To display RadSec server statistics

1 Display RadSec server statistics:

```
radsec show statistics
```

To display RadSec attributes

2 Display RadSec attributes:

```
radsec show
```

—end—

Example

This example shows the output from the radsec show statistics command.

```
> radsec show statistics
+--------------------- RADSEC SERVER STATISTICS ----------------------------+
| No Entries             |                                                  |
+------------------------+--------------------------------------------------+

> radsec show
+------------------------- RADSEC ATTRIBUTES --------------------+
| Parameter                         | Value                      |
+-----------------------------------+----------------------------+
| RadSec Admin State                | Disabled                   |
| RadSec Oper State                 | Disabled                   |
+-----------------------------------+----------------------------+
| Timeout                           | 6s                         |
| Search Method                     | Priority                   |
| Minimum TLS Version               | TLSv1.1                    |
| Greylist Timeout                  | 10m                        |
| Device Certificate Name           | test                       |
| Device Certificate/Key            | Ok                         |
| Device Certificate [SHA-1]        | FA:78:91:FC:61:11:1D:F6... |
| Check Peer Certificate            | Enabled                    |
| Check Peer IP/Hostname            | Disabled                   |
| Check Peer Fingerprint            | Enabled                    |
| Check Cert Time Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| User Accounting Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| OCSP                              |                            |
|     Admin State                   | Disabled                   |
|     Responder Preference          | aia                        |
|     Default Responder             |                            |
|     Nonce                         | On                         |
+-----------------------------------+----------------------------+
+----------------- RADSEC USER LOGIN SERVER TABLE -------------------------+
| IP Address         | HostName         |Pri|Port | State   |Used|Greylist |
|                    |                  |   |     |Adm|Oper |Last|Remaining|
+--------------------+------------------+---+-----+---+-----+----+---------+
| No Entries         |                  |   |     |   |     |    |         |
+--------------------+------------------+---+-----+---+-----+----+---------+

+------------------- RADSEC USER LOGIN ACCOUNTING SERVER TABLE ------------+
| IP Address         | HostName         |Pri|Port | State   |Used|Greylist |
|                    |                  |   |     |Adm|Oper |Last|Remaining|
+--------------------+------------------+---+-----+---+-----+----+---------+
| No Entries         |                  |   |     |   |     |    |         |
+--------------------+------------------+---+-----+---+-----+----+---------+
```

Procedure 9-11
Displaying Secure RADIUS user statistics

You can display Secure RADIUS (RadSec) statistics and configuration.

Step **Action**

To display RadSec user login statistics

1 Display RadSec user login statistics:

```
radsec user-login show statistics
```

To display RadSec user login server statistics

2 Display RadSec user login server statistics:

```
radsec user-login show server <server> statistics
```

To display user RadSec user accounting statistics

3 Display RadSec user login accounting statistics:

```
radsec user-acct show statistics
```

To display user RadSec user accounting server statistics

4 Display RadSec user login server statistics:

```
radsec user-acct show server <server> statistics
```

—end—

Example

This example shows sample output for the RadSec show server statistics command.

```
> radsec show 10.121.240.170 statistics
+--------------------- RADSEC SERVER 1 STATISTICS ---------------------+
| Server IP Address      | 10.121.240.170                             |
| Hostname               | 10.121.240.170                             |
+------------------------+----------------------+----------------------+
|                        | User Login           | User Acct            |
+------------------------+----------------------+----------------------+
| Connection Attempts    | 9                    | 4                    |
| Successful Connections | 3                    | 3                    |
| Failed TCP Connections | 2                    | 0                    |
| Failed TLS Connections | 4                    | 1                    |
| Timed Out Connections  | 1                    | 0                    |
| Unexpected Closes      | 1                    | 0                    |
| Closed Connections     | 2                    | 3                    |
+------------------------+----------------------+----------------------+
| Radius Requests        | 3                    | 3                    |
| Access Accepts         | 2                    | 0                    |
| Access Rejects         | 0                    | 0                    |
| Access Challenges      | 0                    | 0                    |
| Responses              | 0                    | 3                    |
| Malformed Responses    | 0                    | 0                    |
| Bad Authenticators     | 0                    | 0                    |
| Unknown Types          | 0                    | 0                    |
| Packets Dropped        | 0                    | 0                    |
+------------------------+----------------------+----------------------+
```

This example shows sample output for the user-acct show statistics command.

```
> radsec user-acct show
+------------------------- RADSEC ATTRIBUTES --------------------+
| Parameter                         | Value                      |
+-----------------------------------+----------------------------+
| RadSec Admin State                | Disabled                   |
| RadSec Oper State                 | Disabled                   |
+-----------------------------------+----------------------------+
| Timeout                           | 6s                         |
| Search Method                     | Priority                   |
| Minimum TLS Version               | TLSv1.1                    |
| Greylist Timeout                  | 10m                        |
| Device Certificate Name           | test                       |
| Device Certificate/Key            | Ok                         |
| Device Certificate [SHA-1]        | FA:78:91:FC:61:11:1D:F6... |
| Check Peer Certificate            | Enabled                    |
| Check Peer IP/Hostname            | Disabled                   |
| Check Peer Fingerprint            | Enabled                    |
| Check Cert Time Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| User Accounting Admin State       | Enabled                    |
+-----------------------------------+----------------------------+
| OCSP                              |                            |
|     Admin State                   | Disabled                   |
|     Responder Preference          | aia                        |
|     Default Responder             |                            |
|     Nonce                         | On                         |
+-----------------------------------+----------------------------+
+-------------- RADSEC USER LOGIN ACCOUNTING SERVER TABLE -----------------+
| IP Address     | HostName           |Pri|Port | State   |Used|Greylist...|
+----------------+--------------------+---+-----+---+-----+----+-----------+
| 10.121.240.170 | 10.121.240.170     |1  |2083 |Ena|Dis  |    |0          |
+----------------+--------------------+---+-----+---+-----+----+-----------+
```

Procedure 9-12
Clearing Secure RADIUS statistics

You can clear Secure RADIUS statistics manually.

Step **Action**

Clear user login statistics

1 Clear Secure RADIUS user login statistics:

```
radsec user-login clear statistics
```

Clear user account statistics

2 Clear Secure RADIUS user account statistics:

```
radsec user-acct clear statistics
```

—end—

Procedure 9-13
Configuring TACACS+ authentication

You can

- enable multi-factor authentication
- configure TACACS+ authentication
- enable or disable TACACS+ authentication
- remove a TACACS+ authentication server
- set TACACS+ authorization server attributes
- set TACACS+ authorization server attributes to default
- clear TACACS+ authorization server attributes
- display TACACS+ authorization server attributes

Note: A notification/trap is generated if the authentication fails because the client is unable to reach the TACACS server.

Step **Action**

Enable multi-factor authentication

1 Enable multi-factor authentication:

```
tacacs authentication set enhanced multi-factor on
```

To configure TACACS+ authentication

2 Configure authentication:

```
tacacs authentication add server <IP address or host
name[1..63] priority <NUMBER: 1..8] tcp-port <NUMBER:
1..65535>
```

where

server <IP address or host name[1..63>	is the TACACS+ server IP address or hostname.
priority <NUMBER: 1..8>	is the priority of the TACACS+ server.
tcp-port <NUMBER: 1..65535>	is the TCP port of TACACS+ server. The default value is 49.

To enable or disable TACACS+ authentication

3 Configure authentication:

```
tacacs authentication <enable|disable> server <IP address
or host name[1..63]
```

To remove a TACACS+ authentication server

4 Remove an authentication server:

```
tacacs authentication remove server <IP address or host
name[1..63]
```

To set TACACS+ authentication server attributes

5 Set authentication attributes:

```
tacacs authentication set server <IP address or host
name[1..63] priority <NUMBER: 1..8> tdp-port <NUMBER:
1..65535>
```

To set TACACS+ authentication server attributes to default

6 Set authentication attributes to default:

```
tacacs authentication unset server <IP address or host
name[1..63] tdp-port <NUMBER: 1..65535>
```

To clear TACACS+ authentication server attributes

7 Set authentication attributes:

```
tacacs authentication clear server <IP address or host
name[1..63] statistics
```

To display TACACS+ authentication server attributes

8 Display authentication attributes:

```
tacacs authentication show
```

—end—

Procedure 9-14
Configuring TACACS+ authorization

This procedure shows how to configure TACACS+.

In multi-factor authentication, the client prompts for the username, and then lets the server direct all additional prompts.

Step **Action**

To configure TACACS+ authorization

1 Configure authorization:

```
tacacs authorization add server <IP address or host
name[1..63] priority <NUMBER: 1..8] tcp-port <NUMBER:
1..65535>
```

where

server <IP address or host name[1..63>	is the TACACS+ server IP address or hostname.
priority <NUMBER: 1..8>	is the priority of the TACACS+ server.
tcp-port <NUMBER: 1..65535>	is the TCP port of TACACS+ server. The default value is 49.

To enable or disable TACACS+ authorization

2 Configure authorization:

```
tacacs authorization <enable |disable> server <IP address
or host name[1..63]
```

To remove a TACACS+ authorization server

3 Remove an authorization server:

```
tacacs authorization remove server <IP address or host
name[1..63]
```

To set TACACS+ authorization server attributes

4 Set authorization attributes:

```
tacacs authorization set server <IP address or host
name[1..63] priority <NUMBER: 1..8> tdp-port <NUMBER:
1..65535>
```

To set TACACS+ authorization server attributes to default

5 Set authorization attributes to default:

```
tacacs authorization unset server <IP address or host
name[1..63] tdp-port <NUMBER: 1..65535>
```

To clear TACACS+ authorization server attributes

6 Set authorization attributes:

```
tacacs authorization clear server <IP address or host
name[1..63] statistics
```

To display TACACS+ authorization server attributes

7 Display authorization attributes:

```
tacacs authorization show
```

—end—

Example

This example creates 3 TACACS+ servers to be used for authentication, sets the global parameters for using TACACS+ authentication, and then enables AAA.

```
> tacacs add server 10.10.10.100
> tacacs add server 10.10.10.200
> tacacs enable
> tacacs set secret fe:83:7e:21:e1:1c:10:2f:22:44 timeout 2
> tacacs set privilegelvlrw 3
> tacacs set server 10.10.10.200 priority 1
> tacacs authentication enable
> tacacs authorization enable
> tacacs accounting enable
> tacacs set privilegelvldiag 13
> tacacs show

+---------- TACACS+ ATTRIBUTES ---------+
| Parameter                  |  Value   |
+----------------------------+----------+
| Admin State                | Enabled  |
| Oper State                 | Enabled  |
+----------------------------+----------+
| Authentication Admin State | Enabled  |
| Enhanced Multi-Factor Auth | off      |
| Authorization Admin State  | Disabled |
| Accounting Admin State     | Disabled |
| Accounting Session         | off      |
| Accounting Command         | off      |
| Syslog Admin State         | Disabled |
+----------------------------+----------+
| Timeout                    | 6        |
| Key                        | ******** |
| Minimum Key Length         | 8        |
| Search Method              | Priority |
+----------------------------+----------+
| Admin Priv Level           | 2        |
| RW-Create Priv Level       | 10       |
| Diag Priv Level            | 15       |
+----------------------------+----------+
+----------------------- TACACS+ GLOBAL SERVER TABLE -----------------+
| IP Address            | HostName        |Pri |TCP  |Admin|Oper |Last|
|                       |                 |Port|State|State|Used |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
| No Entries            |                 |    |     |     |     |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
+------------------- TACACS+ AUTHENTICATION SERVER TABLE -------------+
| IP Address            | HostName        |Pri |TCP  |Admin|Oper |Last|
|                       |                 |Port|State|State|Used |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
| No Entries            |                 |    |     |     |     |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
+------------------- TACACS+ AUTHORIZATION SERVER TABLE --------------+
| IP Address            | HostName        |Pri |TCP  |Admin|Oper |Last|
|                       |                 |Port|State|State|Used |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
| No Entries            |                 |    |     |     |     |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
+------------------- TACACS+ ACCOUNTING SERVER TABLE -----------------+
| IP Address            | HostName        |Pri |TCP  |Admin|Oper |Last|
|                       |                 |Port|State|State|Used |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
| No Entries            |                 |    |     |     |     |    |
+-----------------------+-----------------+----+-----+-----+-----+----+
```

Procedure 9-15
Configuring TACACS+

Configure TACACS+ for authentication, as well as command line approval. Users can only execute commands that are approved by the TACACS server.

> ***Note:*** A notification/trap is generated if the authentication fails because the client is unable to reach the TACACS server.

Step **Action**

1 Configure the list of TACACS+ servers:

```
tacacs add server <IP address or host name[1..63]>
priority <NUMBER: 1..8> tcp-port <NUMBER: 1..65535>
```

where

server <IP address or host name[1..63>	is the TACACS+ server IP address or hostname.
priority <NUMBER: 1..8>	is the priority of the TACACS+ server.
tcp-port <NUMBER: 1..65535>	is the TCP port of TACACS+ server. The default value is 49.

2 Enable TACACS+ globally:

```
tacacs enable
```

3 Set the global TACACS+ server attributes:

```
tacacs set server <server> priority <NUMBER: 1..8> tcp-
port <NUMBER: 1..65535>
```

where

<server>	is the configured TACACS+ server IP address or hostname.
priority <NUMBER: 1..8>	is the TACACS+ server priority.
tcp-port <NUMBER: 1..65535>	is the TCP port of the TACACS+ server. The default value is 49.

4 Set TACACS+ attributes:

```
tacacs set key <Password String[2..64]> keyminlen
<NUMBER: 2..64> timeout <SECONDS: 1..30>
privilegelvladmin <NUMBER: 2..13> privilegelvlrw <NUMBER:
3..14> global-servers <on | off> search-method <priority
| cached>
```

where

key <Password String[2..64> is the TACACS+ key.

keyminlen <NUMBER: 2..64> is the minimum length of the TACACS+ key.

timeout <SECONDS: 1..30> is the response time from the TACACS+ server. The default value is 6 seconds.

privilegelvladmin <NUMBER: 2..13> is the read-write privilege level. The default value is 2.

privilegelvlrw <NUMBER: 3..14> is the read-write-create privilege level. The default value is 10.

global-servers <on | off> indicates whether to use global server.

search-method <priority | cached> sets the search method for TACACS+ servers.

5 Enable authentication:

```
tacacs authentication enable
```

6 Enable authorization:

```
tacacs authorization enable
```

7 Enable accounting:

```
tacacs accounting enable
```

8 Enable or disable Syslog.

```
tacacs syslog enable
```

9 (Optional) Verify TACACS+ configurations.

```
tacacs show
```

—end—

Procedure 9-16
Configuring TACACS+ and RADIUS user accounting

You can configure TACACS+ and RADIUS user accounting with these settings:

- default — RADIUS accounting is used for users authenticated by RADIUS. TACACS+ accounting can be used for users authenticated by TACACS+.
- radius — RADIUS accounting is used regardless of whether the user is authenticated by RADIUS, TACACS+ or Local.
- tacacs — TACACS+ accounting is used regardless of whether the user is authenticated by TACACS+, RADIUS or Local.
- radsec — RADSEC accounting is used regardless of whether the user is authenticated by RADIUS, TACACS+ or Local.

Step **Action**

1 Configure the user accounting setting:

```
user acct set method <default|radius|tacacs|radsec>
```

where

method <default | radius | tacacs|radsec>	selects the user accounting method as default, radius, tacacs or radsec.

—end—

Procedure 9-17
Displaying TACACS+ and RADIUS user accounting

You can display TACACS+ and RADIUS user accounting settings.

Step **Action**

1 Display the user accounting settings:

```
user acct show
```

—end—

Example

This example shows the output from the user acct show command.

```
> user acct show

+----- ACCOUNTING PROVIDER ------+
| Value     | Admin     | Oper     |
+----------+----------+----------+
| Method    | default   | default  |
+----------+----------+----------+
```

Procedure 9-18
Configuring authentication providers

Three methods of user authentication are supported: local, RADIUS, and TACACS+, and separate authentication methods can be set for the serial port and remote access. By default, the local user database only is used for authentication.

You can configure the device to use a backup authentication method and priority. The backup authentication method is only used if the primary authentication method does not complete because a server is not available (not configured, not enabled, or failed to contact as in a communication error). If the server is contacted and the authentication is denied (not allowed), the secondary method is not called.

For a given authentication method, the scope defines the method called dependent upon the source of the login attempt. For a scope policy equal to "remote", the authentication method is only called for login attempts originating from either the local or remote management interfaces. For a scope policy equal to "serial", the authentication method is only called for login attempts originating from the serial port. For a scope policy of "all", the authentication method is called for all management interfaces, remote, local, and serial. In all cases, the priority backup authentication rules described above apply.

Step **Action**

1 Set the authentication scope, priority, and method:

```
user auth set {priority <NUMBER: 1..3>} {method
<none|local|radius|tacacs>} [scope <all|serial|remote>]
```

where

priority <NUMBER: 1..3>	is the authorization priority.
method <nonellocall radiusltacacs>	is the authorization method.
scope <alllseriall remote>	is the authorization scope.

—end—

Example

You can specify TACACS as the only authentication method for the local and remote interfaces and only use local authentication for serial port connections. If the TACACS servers do not return a response, the local authentication method is not used on the local and remote interfaces. Local authentication is used only for serial port login attempts.

```
> user auth set priority 1 method tacacs scope remote
> user auth set priority 2 method local scope serial
```

Also, you can specify TACACS authentication to be used on the local and remote interfaces and use local authentication for both scopes (this only happens on the local and remote interfaces if the TACACS servers cannot be reached).

```
> user auth set priority 1 method tacacs scope remote
> user auth set priority 2 method local scope all
```

Procedure 9-19
Displaying authentication providers and statistics

Display authentication providers and statistics.

Step	Action
1	Display authentication providers and statistics: `user auth show`

—end—

Example

This example shows sample output for the user auth show command.

```
> user auth show
+----------------------------------------------------------------------+
| Priority | Method   |  Called | Success | Failure | Skipped | Scope  |
+----------+----------+---------+---------+---------+---------+--------+
| 1        | local    |       6 |       5 |       1 |       0 |    all |
+----------+----------+---------+---------+---------+---------+--------+
```

Procedure 9-20
Clearing authentication statistics

Clear authentication statistics.

Step **Action**

1 Clear authentication statistics:

```
user auth clear [priority <NUMBER 1..3>]
```

where

priority <NUMBER 1..3>	is the authorization priority.

—end—

Example

This example shows the output from the user auth show command.

```
> user auth show
+------------------- AUTHORIZATION PROVIDERS --------------------------+
| Priority | Method   |  Called | Success | Failure | Skipped | Scope  |
+----------+----------+---------+---------+---------+---------+--------+
| 1        | local    |      53 |      46 |       7 |       0 |    all |
+----------+----------+---------+---------+---------+---------+--------+
> user auth clear
> user auth show
+------------------- AUTHORIZATION PROVIDERS --------------------------+
| Priority | Method   |  Called | Success | Failure | Skipped | Scope  |
+----------+----------+---------+---------+---------+---------+--------+
| 1        | local    |       0 |       0 |       0 |       0 |    all |
+----------+----------+---------+---------+---------+---------+--------+
```

Procedure 9-21
Removing authentication methods

Remove authentication methods.

Step **Action**

1 Remove an authentication method:

```
user auth set method none [priority <NUMBER 1..3>]
```

where

priority <NUMBER 1..3> is the authorization priority.

—end—

Example

In the following example, all three authentication methods are configured on the device (radius, tacacs, and local). The removal of each (to set the configuration back to the default value of *local*), is performed by removing Priority Method 1. Once this has been executed, the priority method is automatically reset on the system.

```
user auth set method none priority 1
```

This example shows the output of the user auth show command on the device.

```
> user auth show
+----------------------- Authorization Providers ----------------------+
| Priority | Method    |  Called | Success | Failure | Skipped | Scope  |
+----------+----------+---------+---------+---------+---------+--------+
| 1        | radius    |       0 |       0 |       0 |       0 |    all |
| 2        | tacacs    |       0 |       0 |       0 |       0 |    all |
| 3        | local     |       0 |       0 |       0 |       0 |    all |
+----------+----------+---------+---------+---------+---------+--------+
```

Removing Priority 1 once again leaves the system with only *local* as the authorization method.

```
> user auth set method none priority 1
```

This example shows the output of the user auth show command on the device.

```
> user auth show
+----------------------- Authorization Providers ----------------------+

| Priority | Method    |  Called | Success | Failure | Skipped | Scope  |

+----------+----------+---------+---------+---------+---------+--------+

| 1        | tacacs    |       0 |       0 |       0 |       0 |    all |

| 2        | local     |       0 |       0 |       0 |       0 |    all |

+----------+----------+---------+---------+---------+---------+--------+

> user auth set method none priority 1
> user auth show
+----------------------- Authorization Providers ----------------------+
| Priority | Method   |  Called | Success | Failure | Skipped | Scope  |
+----------+----------+---------+---------+---------+---------+--------+
| 1        | local    |       0 |       0 |       0 |       0 |    all |
+----------+----------+---------+---------+---------+---------+--------+
```

Secure communications and infrastructure

Secure communications and infrastructure is provided by means of

SSH

Secure Shell (SSH) provides remote log on and SFTP file transfers. Intended as a more secure replacement of Telnet, SSH verifies and grants access to login requests by encrypting user ID and passwords. SSH/SFTP is supported over IPv4 and IPv6.

> ***Note:*** When a Ciena device encounters Telnet/SSH session requests quickly and back-to-back in a short period of time, the Telnet/SSH server on the device actively refuses connections to prevent Denial of Service (DoS) attacks. Automatic provisioning systems that provision devices with rapid, successive Telnet/SSH session connections may trigger this DoS protection. To avoid session denial, do not request Telnet/SSH provisioning sessions within 10 seconds of each other.

SSH also supports public key based authentication. In public key based authentication, a password is not required: a key pair consisting of a private key and a public key is generated, and then encrypted and stored on the server. The private key must be distributed to the client machine.

There are three separate sets of algorithms that can be configured:

- SSH server algorithm — controls the algorithms that the SSH server, running on an SAOS device, allows when an SSH client tries to connect to an SAOS device.
- SSH client algorithm — deals solely with the algorithms the SSH client and the SAOS device allow when a user is already logged into the SAOS device and they run `ssh client connect ip...` command to establish a connection to a remote server.
- System xftp sftp-client algorithm — consists of a CLI command which allows a user to control the algorithms which the SSH client component of "xftp" uses when establishing an SSH connection with the specified sftp server when making an xftp file transfer. Since, internally, the SFTP component of XFTP is a completely separate component of the "ssh client" and "ssh server" components, this separate "system xftp sftp-client algorithm" is maintained separately. The ssh component of the XFTP is not the same ssh component used for "ssh client" and "ssh server" and it has a limited list of available algorithms that it supports.

Since the private key grants the same access as a password, it must be equally protected. With the key pair generated the private key may optionally be protected with a passphrase. This encrypts the private key. When accessing a server using a passphrase protected private key, the client requests the passphrase.

Multi-factor authentication allows you to configure SSH to require both a password and a private key (which may also require a passphrase). This configuration can be enabled or disabled.

> ***Note:*** This setting only applies to accounts that have public keys installed. It is the user's responsibility to provide proper public keys and maintain/ protect the matching private keys.

The SSH daemon and client need to use a FIPS 140-2 validated cryptographic module operating in FIPS mode. Only FIPS approved ciphers can be used. SSH must be configured to use Message Authentication Codes (MACs) that employ FIPS-140.2 approved cryptographic hash algorithms.

SAOS devices are capable of being FIPS compliant, but they have to be configured for them to be so. FIPS-validated cyphers are only required if you wish to conform to FIPS. See "FIPS" on page 11-3 for more information.

> ***Note:*** Key exchange parameters are for authentication only.

Key exchange parameters

Key exchange parameters are for authentication only.

SSH supports these key exchange parameters from the client:

- Key exchange algorithm (KEX) to be used to generate a one-time session key for authentication and encryption, including:
  - curve25519-sha256@libssh.org
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group-exchange-sha1
  - diffie-hellman-group14-sha1
  - diffie-hellman-group1-sha1
- Encryption algorithm ciphers. Confidentiality is provided with each side proposing the supported encryption algorithm and agreeing upon one. These encryption algorithms are defined for SSH:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - arcfour256
  - arcfour128
  - aes128-gcm@openssh.com
  - aes256-gcm@openssh.com
  - chacha20-poly1305@openssh.com
  - aes128-cbc
  - 3des-cbc
  - blowfish-cbc
  - cast128-cbc
  - aes192-cbc
  - aes256-cbc
  - arcfour
  - rijindael-cbc@lysator.liu.se
- Message Authentication Code (MAC) algorithms. Each side proposes the supported MAC algorithms and they then agree upon one. These algorithms are used in protocol version 2 for data integrity protection. These options are defined for SSH:

  — hmac-md5-etm@openssh.com

  - hmac-sha1-etm@openssh.com
  - umac-64-etm@openssh.com
  - umac-128-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com
  - hmac-ripemd160-etm@openssh.com
  - hmac-sha1-96-etm@openssh.com
  - hmac-md5-96-etm@openssh.com
  - hmac-md5
  - hmac-sha1
  - umac-64@openssh.com
  - umac-128@openssh.com
  - hmac-sha2-256
  - hmac-sha2-512
  - hmac-ripemd160
  - hmac-ripemd160@openssh.com
  - hmac-sha1-96
  - hmac-md5-96

- Public key authentication algorithms including:
  - ssh-dss
  - ssh-rsa
  - ssh-ed25519
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521
  - ssh-ed25519
  - x509v3-sign-dss
  - x509v3-sign-rsa
  - x509v3-ecdsa-sha2-nistp256
  - x509v3-ecds-sha2-nistp384
  - x509v3-ecdsa-sha2-nistp521
  - rsa-sha2-256
  - rsa-sha2-512

> ***Note:*** To enable SSHv2 commands, the Advanced Security feature license must be installed with the `software license install` command.

To access SSH Server, you need to install an SSH version 2 client. The Tested SSH clients table lists tested SSH clients. Other SSH clients may also be compatible but have not been explicitly tested with SAOS.

Table 10-1
Tested SSH clients

Client	Version	Operating system
Bitvise Tunnelier	Version 4.19	Windows
Esh Client	Version 3.2 for Windows	Windows
JellyfiSSH	Version 4.4	MAC OS X
OpenSSH	4.5	Windows
OpenSSH	OpenSSH_3.9p1, OpenSSL 0.9.7a Feb. 19 2003	RedHat Enterprise Linux
OpenSSH	OpenSSH_6.6.1p1 Ubuntu-2ubuntu2, OpenSSL 1.01f 6 Jan 2014 04	Fedora Core 6
OpenSSH	OpenSSH 5.5p1 OpenSSL 1.0.0a-fips 1Jun2010.	Fedora 14 Desktop
Putty SSH	Release 0.58, 0.60, and 0.61	Windows
SecureCRT	Version 5.1.4 (build 285), Version 6.7.1 (build 188), Beta version 6.8.0 (build 167)	Windows
SSH Tectia	Version 5.0.1.79	Windows
WinSCP	Version 4.1.8 (build 415), Version 4.3.3 (build 1340), Version 4.3.4 (build 1428	Windows

SSH procedures are:

- “Configuring SSH server” on page 10-19
- “Configuring SSH server attributes” on page 10-26
- “Adding and removing SSH clients” on page 10-29
- “Disabling the SSH server” on page 10-31
- “Displaying SSH server algorithm configurations” on page 10-33

- “Enabling and disabling an encryption algorithm on the SSH server” on page 10-32
- “Configuring the SSH client priority of an encryption algorithm” on page 10-42
- “Configuring the SSH client priority of an encryption algorithm” on page 10-42
- “Configuring the SSH client priority of a key exchange algorithm” on page 10-44
- “Configuring new host keys for SSH client connection” on page 10-49
- “Displaying SSH client algorithm configurations” on page 10-45
- “Connecting to an SSH client” on page 10-52

Secure copy

Secure copy or SCP securely transfers files between a local host and a remote host. As SCP uses SSH for the transfer it is based on the same security and authentication as SSH. Normally a client initiates an SSH connection to the remote host, and requests an SCP process to be started on the remote server. The remote SCP process can operate in one of two modes:

- source mode — reads files (usually from disk) and sends them back to the client, or
- sink mode — accepts the files sent by the client and writes them (usually to disk) on one remote host

Secure Copy is enabled by installing the Advanced Security license, enabling the SSH server, and adding the correct client IP address to the SSH server.

SFTP and secure copy

SCP can only be used for transferring files and it is non-interactive. This means that everything must be specified on the command line. SFTP allows for more interactive commands to perform tasks such as creating directories, deleting directories and files.

The SFTP protocol allows for a range of operations on remote files. An SFTP client’s extra capabilities compared to an SCP client includes resuming interrupted transfers, directory listings, and remote file removal. As a result, it is simple to implement a GUI SFTP client compared with a GUI SCP client.

SCP and SFTP both use the same SSH encryption during file transfer with the same level of overhead. SCP is usually much faster than SFTP when transferring files, especially on high latency networks. This is because SCP implements a more efficient transfer algorithm, one which does not require waiting for packet confirmations. This leads to faster speed, but it is not possible to interrupt a transfer. Unlike SFTP, SCP transfers cannot be canceled without terminating the session.

Compared to the SCP protocol, which only allows file transfers, the SFTP protocol allows a range of operations on remote files to be performed. An SFTP client can resume interrupted transfers, directory listings, and remote file removal.

SFTP is more platform-independent than SCP. With SCP, the expansion of wildcards specified by the client is up to the server, whereas SFTP avoids this problem. SCP is more frequently implement on UNIX platforms, while SFTP servers are available on most platforms.

SFTP is not FTP run over SSH, but a new protocol designed by the IETF SECSH working group. It is sometimes confused with Simple File Transfer Protocol.

The protocol does not provide authentication and security. It expects the underlying protocol to secure this. SFTP is most often used as a subsystem of SSH protocol version 2 implementations, as it was designed by the same working group. It is possible to run it over SSH-1 or other data streams. Running an SFTP server over SSH-1 is not platform independent as SSH-1 does not support subsystems. An SFTP client willing to connect to an SSH-1 server needs to know the path to the SFTP server binary on the server side.

For uploads, the transferred files may be associated with their basic attributes, such as timestamps. This is an advantage over the common FTP protocol, which does not have the provision for uploads to include the original date/ timestamp attribute without help.

This is the procedure for secure copy:

- “Copying files by means of secure copy” on page 10-53

SFTP/FTP/TFTP

SFTP/TFTP/FTP clients are used to download files from an SFTP/TFTP/FTP server, for example, software images.

Switches also support an SFTP/FTP server to enable external SFTP/TFTP/ FTP clients to download files from the switch. For example, you can store software packages on a device, and then use it as a xFTP server for installing/ upgrading software packages on other devices.

SFTP client

After setting up the SSH server, you can transfer files with an SFTP client. SFTP uses standard file transfer commands for transferring files. SFTP encrypts the user ID, password, and the file and then transfers the information over the SSH server port number.

The Tested SFTP clients table lists tested SFTP clients. Other SFTP clients may also be compatible but have not been explicitly tested.

Table 10-2
Tested SFTP clients

Client	Version	Operating system
Bitvise Tunnelier	Version 4.19	Windows
Esh Client	Version 3.2 for Windows	Windows
JellyfiSSH	Version 4.4	MAC OS X
OpenSSH	Version 4.5	Windows
Putty SSH	Release .58	Windows
SecureCRT	Version 5.1.4 (build 285) - Official Release - September 14, 2006	Windows
SSH Tectia	Version 5.0.1.79	Windows
Nautilus	Version 2.30.1	Ubuntu/Linux/Gnome
WinSCP	Version 4.3.2	Windows

SFTP/FTP/TFTP procedures are:

- "Enabling and disabling the SFTP server" on page 10-54
- "Transferring files with the SFTP client" on page 10-58
- "Transferring files with the FTP client" on page 10-59
- "Transferring files with the TFTP client" on page 10-60

Management interface firewall

The IP firewall provides an additional layer of security. This is done by ensuring that the device is listening for IP traffic only on ports where traffic is allowed. The firewall causes requests to contact the device on other ports to be silently discarded.

The firewall is designed to close all ports and then open only the ports that are active. This protects the network from software that binds to a port and ends up listening on the management network. The firewall drops all packets destined for blocked ports. The IP firewall operates on all DCN ports and the remote management interface. Ports for protocols that are disabled are blocked. Ports are open when the ports are enabled. For protocols such as SSH that can be configured to work on non-default ports, the default port is blocked when a non-default port is configured so that only the currently configured port is open for connections. There are no firewall restrictions on backplane traffic.

This table lists required ports.

Table 10-3
Ports and firewall state

Protocol/Service	Default Port	Default Firewall Status	Notes
SSH Server	TCP port 22	Open	Port can be reconfigured to a non-default value.
Telnet Server	TCP port 23	Open	
SNMP Server	UDP port 161	Open	
SFTP Server	SSH server port	Open	Port open/close is dependent on SSH admin state only.
RADIUS Client	1812	Closed	RADIUS requests originate from the device. RADIUS port does not show as open from the outside world.
TACACS Client	49	Closed	TACACS requests originate from the device. TACACS port does not show as open from the outside world.
DHCP Client	Same as bootp	Closed	DHCP requests originate from the device and does not show up as open from the outside world.
NTP Client	123	Closed	When NTP mode is set to “polling”, the NTP port is closed. When it is set to “broadcast” or “multicast” (IPv6), the firewall is open.
All others	Various	Closed	

MAC tables

When a device receives a packet destined for an unknown destination MAC address, it floods the packet to every connected link. As it receives responses back, devices dynamically learn the association between the source MAC address, port, VLAN, and virtual switch, and then enter the information in the MAC table. Without an Advanced Ethernet (AE) license, the number of learned entries is limited to 4,000. With an installed AE license the number of learned entries supported depends upon the hardware platform. In addition to dynamically learned entries, entries can be statically entered for known source MAC addresses.

This table lists the number of dynamic source MAC addresses and the number of static MAC addresses that are supported by each platform.

Table 10-4
Dynamic and static source MAC addresses per hardware platform

Platform	Number of Dynamic source MAC addresses	Number of static MAC addresses
3903, 3903x, 3904, 3905, 3906	16,000	1024
3926, 3928, 3942	32,000	1024
5142, 5160	128,000	2048

Platforms are capable of learning 15000 source MAC addresses in 3 seconds. Upon reaching the entry limit, source MAC addresses are no longer learned. The system software provides various methods for managing MAC tables, including:

- MAC aging, which automatically removes stale dynamic entries
- Service Access Control (SAC), which controls packet forwarding based on MAC addresses
- MAC learning control, which disables and enables MAC learning on a specific VLAN or virtual switch

> ***Note:*** Because the device learns at line rate, the `flow show mac-addr` command lags behind the hardware when learning at a high rate.

MAC aging

If the number of dynamic MAC address entries, exceeds the maximum, aging removes entries that have been inactive for the specified time limit (configurable from 10 to 1000000 seconds). The default time is 300 seconds and aging is enabled.

> ***Note:*** Static MAC address entries never age out.

When MAC aging is disabled, dynamically-learned MAC addresses remain in the MAC table until flushed by one of these events:

- the flow mac-addr flush command is executed
- the Spanning Tree topology changes
- the link state changes
- the device is rebooted

The MAC aging timer is configured for the entire device: it cannot be set on a virtual switch, VLAN, or port basis. Depending on the location of the device in the network, changing the MAC aging time can cause connectivity issues with critical devices. When changing the MAC aging time, be certain that desirable devices are not inadvertently aged-out.

MAC table procedures are:

- “Managing MAC tables” on page 10-62
- “Enabling and disabling MAC learning control” on page 10-64
- “Displaying the status of MAC learning” on page 10-66

802.1x.

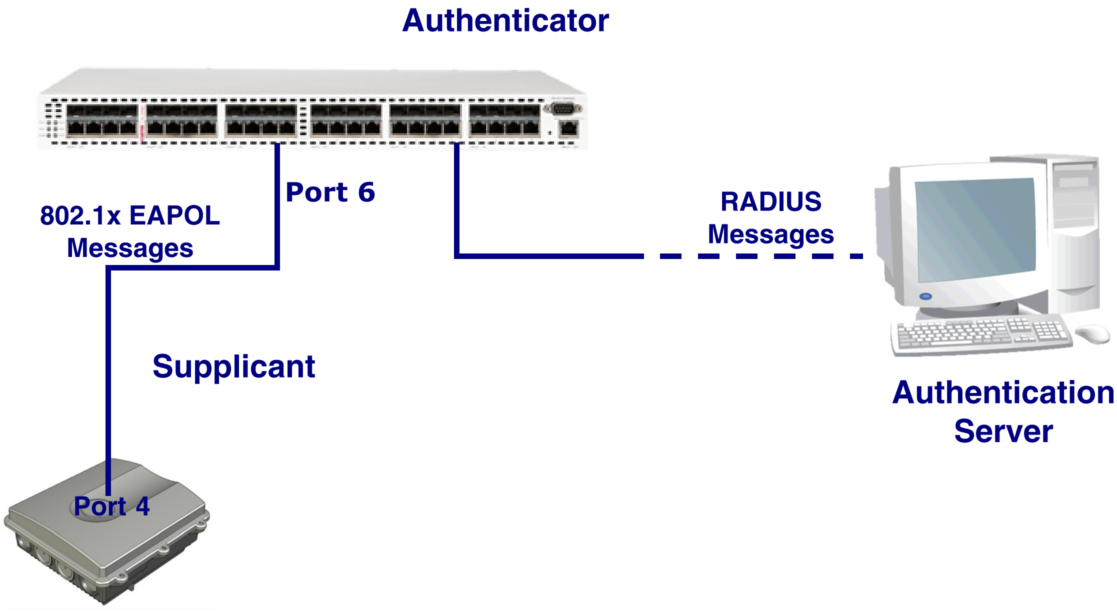
The IEEE 802.1x-2010 standard defines an authentication protocol that uses a centralized authentication server (typically a RADIUS server) to provide port-based and user-based network access control. This provides a method for authenticating customer premise equipment (CPE) and the Switches and Platforms 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 user’s credentials to a pre-entered subscriber database entry and decides whether to allow the device full access to the network.

> ***Note 1:*** To enable IEEE 802.1x security commands, the Advanced-Security feature license must be installed with the `software license install` command.
>
> ***Note 2:*** IEEE 802.1x security commands cannot be used if the device is in MSTP mode, even if MSTP is disabled.

The use of 802.1x with RADIUS authentication differs from standard RADIUS management authentication. 802.1x uses port-based authentication, whereas RADIUS by itself is used to authenticate *users* who are attempting to access a device to change or monitor its configuration. The same RADIUS server can be used for authentication in both instances. This figure shows an example of 802.1x authentication.

Figure 10-1
IEEE 802.1x authentication example



802.1x roles

The 802.1x standard specifies these roles in the authentication process:

- Supplicant
- Authenticator
- Authentication server

Supplicant

The supplicant is the device requesting access to the network. This can be a subscriber device, such as a PC, or a port on a Service Delivery/Aggregation Switch that is connected to another device providing its uplink. In the case of a PC, the PC's network interface card (NIC) is configured for 802.1x authentication using EAP-MD5 or EAP-TLS. When the NIC is enabled, it issues an 802.1x authentication request to a port on the device providing its uplink that is configured as an 802.1x Authenticator. Until the Supplicant is successfully authenticated, only extensible application protocol over LAN (EAPOL) messages from the Supplicant are accepted by the Authenticator port on the uplink device, while other data packets are dropped.

> ***Note:*** If the Supplicant is configured to use DHCP to obtain an IP address, the DHCP request is not passed to the DHCP server until after the Supplicant has successfully authenticated. If the Supplicant does not authenticate, it does not receive an IP address—preventing it from being reached via an uplink or a subscriber connection. A direct serial port connection to the Supplicant device is then required to correct the problem.

Authenticator

The authenticator acts as an intermediary between the 802.1x Supplicant and the RADIUS Authentication Server. It receives the EAPOL formatted authentication request from the Supplicant, encapsulates the authentication request into a RADIUS message, and passes the authentication request to the Authentication (RADIUS) Server. The response from the Authentication Server is sent back to the Authenticator, which forwards the response to the Supplicant. The Authenticator also uses the RADIUS response to determine whether to begin passing regular data traffic to/from the Supplicant.

The port acting as the authenticator can be configured to respond to 802.1x frames as described in this table.

Table 10-5
Authenticator port configurations

Configuration	Description
Auto	Provides 802.1x operation on a port, allowing only EAPOL frames to be sent and received until the client successfully authenticates. Once authenticated, regular traffic is allowed.
Force Authorized	Disables 802.1x and the port is in an authorized state. The port transmits and receives normal traffic without 802.1x-based authentication of the client.
Force Unauthorized	Causes all communications from an 802.1x client to be blocked, preventing the client from authenticating through this port.

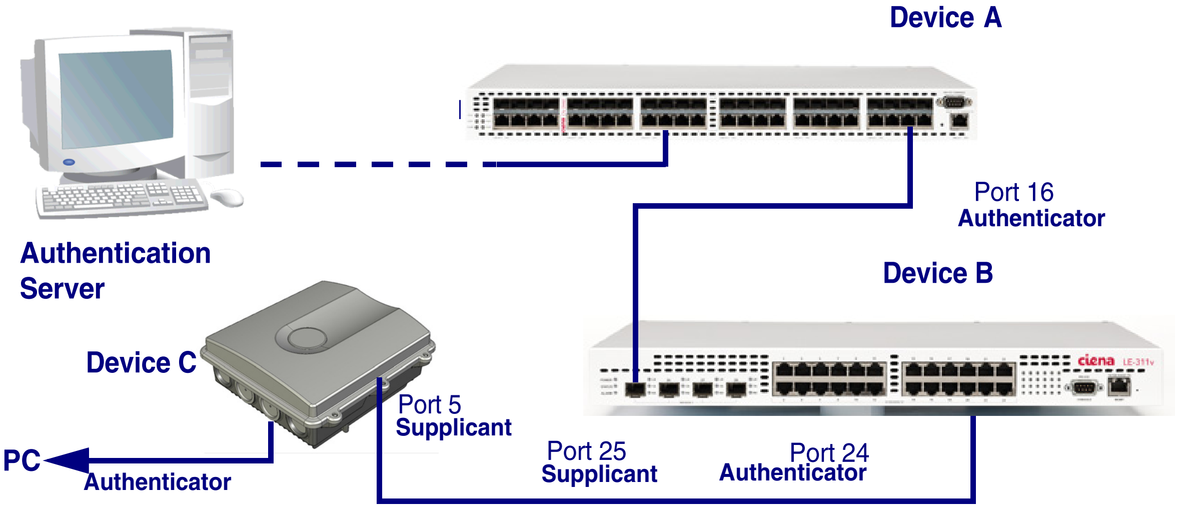
Authentication server

The authentication server receives the RADIUS authentication requests sent from the Authenticator, looks to see if the user’s credentials are in its subscriber data base, and responds with a message to allow or deny network access to the Supplicant. For the authentication to succeed, the Authentication Server must be configured to accept the same encryption type as the Supplicant (currently EAP-MD5 and EAP-TLS are supported).

Deployment example

The IEEE 802.1x deployment example figure illustrates a possible network topology where 802.1x is used. Device A has a connection to an Authentication server that is configured with a list of user names and passwords. Device A port 16 is configured as an Authenticator, and is connected to Device B port 25, which is configured as a Supplicant. When Device B is connected to Device A and is powered on, it sends out EAPOL messages to Device A to begin the authentication process. Device A forms the EAPOL messages into a RADIUS message and forwards the request to the Authentication Server. Once authenticated, Device A port 16 allows regular traffic to ingress from Device B port 25. If Device B port 25 fails to authenticate, regular traffic from that port is blocked, preventing traffic from any devices downstream from reaching the network.

Figure 10-2
IEEE 802.1x deployment example



After Device B port 25 has successfully authenticated, it can pass data from downstream devices that receive their uplink from that port, such as Device C connected to port 24. When Device C connected to Device B is powered on, it sends EAPOL messages out port 5 to Device B port 24, which in turn forms the message into a RADIUS message and forwards it upstream to the Authentication Server. Once Device C has successfully authenticated, Device B port 24 allows regular traffic from Device C to ingress that port.

If a PC is connected to a subscriber port on Device C, the same 802.1x process can be used to authenticate the PC and unblock the port on Device C to provide network access.

Using 802.1x with LACP

802.1x operation controls the state of physical ports, allowing or denying a port access based on its authentication state. Ports that are configured as 802.1x supplicants that are members of a link aggregation group must be authenticated to pass traffic as part of that LACP group.

If a port that is a member of an LACP group becomes unauthenticated during operation, it is removed from the distribution list.

Supplicant and authenticator configuration

For all of the following examples, refer to the drawing for the IEEE 802.1x deployment example. These examples configure only Device A and Device B. Port 16 on Device A is configured as an authenticator and port 25 on Device B as a supplicant. These examples also assume that the proper entries have already been entered on the authentication (RADIUS) server.

As previously described, 802.1x operation comprise three entities: supplicant, authenticator, and authentication server. The supplicant and authenticator are configured on individual physical ports on the devices.

The authentication server is a third-party device that is separately controlled by the network administrator, but must be accessible by the authenticator to authenticate the supplicant. The user name(s) and credentials used by supplicants must be configured on the server. The server must also be configured to use EAP-MD5 or EAP-TLS authentication.

Most authentication servers can be configured to allow multiple supplicants to use the same user credentials to authenticate, but may also require each supplicant to have a unique user name and/or password.

> ***Note:*** The following authenticator and supplicant configuration examples assume that all 802.1x controls are in their default state. Only the required controls are changed to successfully authenticate the supplicant device. Additional configuration changes may be required, depending on the actual network topology.

Authentication verification

The Port Access Entity (PAE) state for the supplicant and the authenticator monitor the current state of authentication. When the supplicant has authenticated, both devices indicate that state.

802.1x procedures are:

- “Enabling and disabling dot1x” on page 10-68
- “Enabling and disabling dot1x authentication” on page 10-69
- “Configuring dot1x authentication port attributes” on page 10-70
- “Displaying dot1x authentication information” on page 10-71
- “Clearing authenticator statistics” on page 10-73
- “Reauthenticating the port” on page 10-74
- “Resetting dot1x authentication port attributes” on page 10-75
- “Configuring the 802.1x supplicant for EAP-MD5” on page 10-76
- “Displaying dot1x global information” on page 10-82

- “Restarting the authenticator or supplicant on a port” on page 10-92
- “Configuring a PC as a supplicant” on page 10-93
- “Troubleshooting 802.1x” on page 10-96

SNMP

SNMP supports secure communications and infrastructure by means of community mapping and the view-based access control model.

SNMP procedures are:

- “Configuring SNMP community mapping” on page 10-97
- “Creating and attaching an SNMPv3 user to an SNMPv3 access entry group” on page 10-101

Vulnerability

A vulnerability assessment identifies, quantifies and prioritizes or ranks vulnerabilities in a system. The Ciena Vulnerability Process (CVP) is applied to all packet networking products.

CVP is an on-going process that is integrated into the product lifecycle process. This process requires weekly monitoring of alerts from Homeland Security National Vulnerability Database (NVD) and US CERT. Vulnerabilities that are identified are analyzed to determine what products and software releases are affected. The risk in each product is also assessed and customers are notified. A remediation plan that includes either a fix or workaround is determined and communicated to the customer.

Vulnerabilities that require a software fix are assigned to the next possible release. Deployment of a resolution consists of a patch, maintenance release, or major release. Ciena takes into consideration a customer’s operational requirements when deploying a resolution.

This table shows how the resolution timeline depends on the severity of the vulnerability.

Table 10-6
Vulnerability timeline

Severity	Notify	Assess	Remediation
Critical	7 days	7 days	Patch/ maintenance release
Major	7 days	7 days	Maintenance release
Minor	30 days	30 days	Next major release

Vulnerability scanning

A vulnerability scanner conducts network reconnaissance, typically carried out by a remote attacker attempting to gain information or access to an unauthorized network. Network reconnaissance exploits network standards and automated communication methods. It determines the types of computers present, and additional information that includes the operating system. This information is analyzed for vulnerabilities that can be exploited to gain access to secure networks and computers. This table describes the vulnerability scans supported by CVP.

Table 10-7
Vulnerability scans

Vulnerability Scans	**Description**
Network Mapper (NMAP)	Attempts to connect to ports to acquire information about which ports are open and what services and operating systems are behind them.
NESSUS	Scans for vulnerabilities that allow a remote hacker to control or access sensitive data, system misconfigurations, default passwords, and denials of service.
Codenomicon	Scans for known and unknown vulnerabilities. Know vulnerabilities are detected by subscribing to vulnerability databases. Unknown vulnerabilities are discovered through fuzzing which discovers unknown vulnerabilities proactively making it easier and faster to fix them.
Open Vas	Scans and manages Open Source vulnerability.
HPING	Scans idle networks and tests firewalls and networks.
Metasploit	Conducts software penetration testing.
Retina	Scans for IT exposures and prioritizes remediation across the enterprise.

Vulnerability scans are done in normal mode for major, minor and maintenance releases. Any issues found are assessed and remedied by means of the CVP. Ciena can provide, if requested, a customer report detailing issues detected by the NMAP, NESSUS and Codenomicon scans.

Procedure 10-1
Configuring SSH server

This procedure configures an SSH server and includes optional steps for configuring X.509 certificates.

Prerequisites

For X.509 user public key authenticate, generate the user's signed public certificate in pem format external to the SAOS switch.

Step	Action

To configure the server

1 Generate the SAOS SSH server host keys:

```
ssh server key generate
```

2 Display the configuration to verify that the value of the Key Status parameter is Generated and that there is a value for the Key Fingerprint parameter in the SSH Attributes table:

```
ssh server show
```

Note: Key generation may take several minutes to complete.

3 Enable the SSH server.

```
ssh server enable
```

4 Display the current configuration to verify that it is enabled and operational:

```
ssh server show
```

5 Save the configuration.

```
configuration save
```

Note: The SSH server now accepts login from an SSH client using a local user name and password.

SSH Server X.509 Host Key:

If support for SSH Server X.509 host key authentication is desired, create and install an SSH Server X.509 Host Key.

6 At an external xFTP server, create a configuration file with the subject name for the device certificate.

7 At the SAOS switch, create a private key, download the certificate configuration file from the xFTP server and generate a certificate signing request (CSR).

```
ssh server certificate csr generate ftp-server <IP
Address> filename <config file> login-id <ftp user>
echoless-password
```

The CSR is uploaded to the ftp server as <filename>.csr

8 At a Certificate Authority or using tools like OpenSSL, sign and install the certificate.

9 Place the signed certificate in pem format on the external xFTP server.

10 At the SAOS switch, install the SSH server to offer the X.509 certificate based host key:

```
ssh server certificate install ftp-server <ip address>
filename <host-certificate> login-id <ftp user> echoless-
password
```

11 (Optional) Restrict the SSH server to offer X.509 certificate based host key:

```
ssh server set x509-host-key only
```

To disable SSH password authentication

12 Use this command to disable SSH password authentication and force only public key authentication (with or without X.509 certificates).

```
ssh server set auth-policy public-key
```

To configure SSH server user public key authentication

13 Install the user’s public key on the SAOS switch from a remote ftp server.

```
ssh server key install user <user> ftp-server <ip address>
login-id <ftp user> echoless password
```

To configure SSH Server X.509 user public key authentication

14 Place the certificate in the root directory of an xFTP server that can be reached by the SAOS switch, along with the CA certificate that signed the user's certificate.

15 Install the user’s certificate:

```
ssh server certificate install user <user> ftp-server <IP
Address> filename <users-certificate> login-in <ftp user>
echoless password
```

16 Install the CA certificate:

```
system security pkix ca install filename <ca-certificate>
ftp-server <ipaddress> login-id <ftp user>
echolesspassword
```

To configure SSH server algorithms

17 Enable or disable SSH server algorithms

```
ssh server algorithm encryption <enable|disable>
<encryption-algorithm>
```

```
ssh server algorithm mac <enable|disable> algorithm <mac-
algorithm>
```

```
ssh server algorithm kex <enable|disable> algorithm <kex-
algorithm>
```

```
ssh server algorithm public-key-authentication
<enable|disable> algorithm <public-key-algorithm>
```

To configure SSH Server X.509 OCSP client

OCSP can optionally be enabled to do real time certificate status checking when validating users X.509 public keys.

18 Enable OCSP checking:

```
ssh server ocsp enable
```

19 Set default OCSP responder:

```
ssh server ocsp set default-responder <responder-url>
```

20 Set OCSP responder first attempt preference:

```
ssh server ocsp set responder-preference <string>
```

To configure SSH Client Algorithms

21 Enable or disable SSH client algorithms

```
ssh client algorithm encryption <enable|disable>
<encryption-algorithm>
```

```
ssh client algorithm mac <enable|disable> algorithm <mac-
algorithm>
```

```
ssh client algorithm kex <enable|disable> algorithm <kex-
algorithm>
```

```
ssh client algorithm host-key-authentication
<enable|disable> algorithm <public-key-algorithm>
```

To configure SSH Client X.509 OCSP client

OCSP can optionally be enabled to do real time certificate status checking when validating users X.509 public keys.

22 Enable or disable OCSP checking:

```
ssh client ocsp enable|disable
```

23 Set default OCSP responder:

```
ssh client ocsp set default-responder <responder-url>
```

24 Set default OCSP responder first attempt preference:

25
```
ssh client ocsp set responder-preference <responder-url>
```

To enable public key authentication

26 On your SSH client, generate the user public and private keys following the instructions per your SSH client, and place the public key on an xFTP server.

Note 1: The format for the public key file name must be .pk2 or .pub. For example, the key file name for user must be user.pk2 or user.pub.

Note 2: The format of key files must be as specified in the AUTHORIZED_KEYS FILE FORMAT section of the OpenBSD man page for "sshd": *https://man.openbsd.org/sshd*.

27 Provision user public keys manually on the switch:

```
ssh server install key user <username> {filename
<String>}
{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

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use 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 sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

28 Verify the installation:

```
ssh server show key
```

Note: If key status indicates that the shell user account is not created, you need to create an account for that user before they can log in. The shell user account must be created with a password.

—end—

Example

This example shows the output from the ssh server show command.

```
> ssh server show
+------------------------------- SSH ATTRIBUTES ---------------------------+
| Parameter               | Value
|-------------------------+------------------------------------------------+
| Admin State             | Disabled                                       |
| Oper State              | Disabled                                       |
| Listener Address Group  | all                                            |
| Listener Port           | 22                                             |
| Authentication Retries  | 3                                              |
| Client Alive Interval   | 0 seconds                                      |
| Client Alive Count      | 0                                              |
| FIPS-1402 Mode          | off                                            |
| Login Grace Time        | 120 seconds                                    |
| Max Shared Sessions     | 10                                             |
| Multi Factor Auth       | off                                            |
| Authentication Policy   | all                                            |
| Rekey Limit             | default                                        |
| Rekey Timeout           | none                                           |
| Strict Modes            | off                                            |
| TCP Forwarding          | on                                             |
| TCP Keep Alive          | on                                             |
| X509 Host Key           | enabled                                        |
| Host Certificate Status | Not Installed                                  |
| Key Status              | Generated                                      |
| Key Type                | rsa2048                                        |
| Key Fingerprint [MD5]   | fc:bf:b9:4c:09:78:41:9a:db:cf:23:50:19:74:27:b9|
+-------------------------+------------------------------------------------+

+------------------------ SSH LISTENER ADDRESS ------------------------+
| Listen Address                                     | Interface       |
+----------------------------------------------------+-----------------+
| 0.0.0.0                                            | all             |
| ::                                                 | all             |
+----------------------------------------------------+-----------------+

+-----------------------------ALLOWED CLIENTS ----------------------+
| IP Address                                  | HostName | State    |
+---------------------------------------------+----------+----------+
| No Entries                                  |          |          |
+---------------------------------------------+---------------------+

+--------- SSH GLOBAL STATUS --------+
| Attribute            | Value       |
+----------------------+-------------+
| Active Limited Users | 0           |
| Active Admin Users   | 0           |
| Active Super Users   | 0           |
| Total Active Users   | 0           |
+----------------------+-------------+
```

Example config file:

```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no
```

```
[ req_distinguished_name ]
C                       = US
ST                      = Maryland
L                       = Hanover
O                       = YourCompany
OU                      = YourDepartment
CN                      = 8700SSHServer
emailAddress            = RadSecClient@none.invalid
```

This example configures SSH server algorithms.

```
> ssh server algorithm encryption enable algorithm 3des-cbc
> ssh server algorithm encryption disable algorithm arcfour
> ssh server algorithm mac enable algorithm hmac-sha2-256
> ssh server algorithm mac disable algorithm hmac-md5
> ssh server algorithm kex enable algorithm diffie-hellman-group-exchange-
sha256
> ssh server algorithm kex disable algorithm diffie-hellman-group14-sha1
> ssh server algorithm public-key-authentication enable algorithm x509v3-
ecdsa-sha2-nistp384
> ssh server algorithm public-key-authentication disable algorithm ssh-
ed25519
```

This example configures SSH client algorithms.

```
> ssh client algorithm encryption enable algorithm 3des-cbc
> ssh client algorithm encryption disable algorithm arcfour
> ssh client algorithm mac enable algorithm hmac-sha2-256
> ssh client algorithm mac disable algorithm hmac-md5
> ssh client algorithm kex enable algorithm diffie-hellman-group-exchange-
sha256
> ssh client algorithm kex disable algorithm diffie-hellman-group14-sha1
> ssh client algorithm public-key-authentication enable algorithm x509v3-
ecdsa-sha2-nistp384
> ssh client algorithm public-key-authentication disable algorithm ssh-
ed25519
```

This example configures SSH Server X.509 OCSP client.

```
> ssh client ocsp set default-responder http://10.1.1.100:8080
```

This example sets default OCSP responder.

```
> ssh server ocsp set default-responder http://10.1.1.100:8080
```

This example sets the OCSP responder first attempt preference.

```
> ssh server ocsp set responder-preference http://10.1.1.100:8080
```

This example configures SSH Server X.509 OCSP client.

```
> ssh server ocsp enable
> ssh server ocsp set default-responder http://10.1.1.100
> ssh server ocsp set responder-preference http://10.1.1.100
```

This example configures SSH Client Algorithms.

```
> ssh client algorithm encryption enable algorithm 3des-cbc
> ssh client algorithm encryption disable algorithm arcfour
> ssh client algorithm mac enable algorithm hmac-sha2-256
> ssh client algorithm mac disable algorithm hmac-md5
> ssh client algorithm kex enable algorithm diffie-hellman-group-exchange-
sha256
> ssh client algorithm kex disable algorithm diffie-hellman-group14-sha1
> ssh client algorithm host-key-authentication enable algorithm x509v3-ecdsa-
sha2-nistp384
> ssh client algorithm host-key-authentication disable algorithm ssh-ed25519
```

This example configures SSH Client X.509 OCSP client.

```
> ssh client ocsp enable
> ssh client ocsp set default-responder http://10.1.1.100:8080
ssh client ocsp set responder-preference http://10.1.1.100:8080
```

Procedure 10-2
Configuring SSH server attributes

You can configure:

- the number of times the SSH server attempts authentication
- the number of client-alive interval messages
- the number of client-alive count messages
- the client timeout interval
- the listener address group
- the port that listens for SSH requests
- the login grace time
- the maximum shared sessions
- multi-factor authorization
- the rekey limit
- the rekey-timeout
- strict-mode - whether the system checks the modes and ownership of the user's files and home directory before accepting login
- tcp forwarding and keep alive
- 509 host key
- listener address group
- whether the system sends keepalive messages to the other side of the connection

The number of times the SSH server attempts authentication is set by means of the authentication-retries attribute. The authentication retry counter is incremented when any authentication method fails, even in the same login cycle. For example, with authentication-retries set to 3, when the SSH client fails to authenticate using an RSA public key, each attempt increments the authentication-retries counter and only one prompt for a user name and password occurs for that login cycle.

Because an SSH client attempts to log in with keys before using the password authentication method, Ciena recommends a minimum value of 2 for the authentication-retries setting.

Step **Action**

1 Display available ssh server set attributes:

```
ssh server set?
```

where

authentication-retries <NUMBER: 1..3>	maximum retries (Default: 3)
client-alive-count <NUMBER: 0..10>	specifies the number of client alive messages (Default: 0)
client-alive-interval <SECONDS: 0..2147483647>	specifies the client timeout interval (Normal default: 0 seconds, Enhanced security default: 60 seconds)
listener-address-group <String>	addresses group to listen for SSH connections (Default: all)
listener-port <NUMBER: 22..65535>	port to listen for SSH connections (Default: 22)
login-grace-time <SECONDS: 0..2147483647>	specifies the login grace timeout (Default: 120 seconds)
max-shared-sessions <NUMBER: 1..10>	set max sessions per network connection (Normal default: 10, Enhanced security default: 1)
multi-factor-auth <String>	turns ssh multi factor authentication on or off (Normal default: off)
rekey-limit <String>	specifies the number of bytes that is transmitted before the session key is renegotiated (Normal default: default, Enhanced security default: 1G)
rekey-timeout <duration: number/time format N[yMwdhms] e.g. 1h10m3s for 1 hour, 10 minutes and 3 seconds>	specifies the max time to pass before the session key is renegotiated (Normal default: 0, Enhanced security default: 1h)
strict-modes <String>	sets support for ssh strict mode (Normal default: off, Enhanced security default: on)
tcp-forwarding <String>	turns TCP forwarding on or off (Normal default: on, Enhanced security default: off)

where

tcp-keepalive <String>	turns TCP keep alive on or off (Normal default: on, Enhanced security default: off)
auth-policy <String>	sets the authentication policy
x509-host-key <String>	sets x509 host key usage (default: enabled)

To ensure that listening starts on the new listener port:

2 Disable SSH server:

```
ssh server disable
```

3 Enable SSH server:

```
ssh server enable
```

Example

This example sets the SSH authentication retries to 2 and specifies a listener port.

```
> ssh server set authentication-retries 2 listener-port 1005
```

—end—

Procedure 10-3
Adding and removing SSH clients

Add clients to restrict access to the IP addresses in the client list. If you do not want to accept a connection from an SSH client, you can remove the SSH client from the client list. The default configuration allows any IP address to connect.

Step **Action**

To add an IP address for each client

1 Add an IP address for each client:

```
ssh server add {[client <ip-host-str | IPADDRESS in CIDR
notation>]
```

where

client <ip-host-str | IPADDRESS in CIDR notation>>	is the valid client IP, hostname, or subnet mask in CIDR notation on which the connection is accepted. By default, connection is accepted for all IP addresses. When one or more clients have been added, then access is restricted to only those that been added.

To remove a client

2 Remove any clients from which you do not want to accept a connection.

```
ssh server remove [client <ip-host-str | IPADDRESS in CIDR
notation>]
```

where

client <client>	is the valid client IP, hostname, or subnet mask in CIDR notation in which you are removing a client from which the device does not intend to accept any more connections. In the case of removing the last client, then connections are allowed from all clients.

—end—

Example

This example adds a client with the IP address 192.0.2.1.

```
ssh server add client 192.0.2.1
```

This example removes a client with the IP address 192.0.2.1.

```
ssh server remove client 192.0.2.1
```

Procedure 10-4
Enabling SSH server

Enable the SSH server globally when the network operator intends users to log into the SAOS switch by means of SSH. The default is disable.

> ***Note:*** Disabling the SSH server also disables SFP and SCP servers since these services operate on top of SSH.

Step	Action
1	Enable SSH server: `ssh server enable`

—end—

Procedure 10-5
Disabling the SSH server

Disable the SSH server globally when the network operator no longer intends to log into the switch by means of SSH. The default is disable.

> ***Note:*** Disabling the SSH server also disables SFP and SCP servers since these services operate on top of SSH.

Step	Action
1	Disable SSH server: `ssh server disable`

—end—

Procedure 10-6
Enabling and disabling an encryption algorithm on the SSH server

Enable or disable an encryption algorithm on the SSH server according to the network operator security plan. You must have administrative user privileges to perform this procedure.

Step **Action**

1 Enable or disable an encryption algorithm:

```
ssh server algorithm encryption <enable|disable>
algorithm <encryption-algorithm>
```

where

enable|disable enables the encryption algorithm

encryption-algorithm is the specific algorithm.

kex-algorithm enables or disables the key exchange algorithm.

—end—

Example

This example shows the output from the ssh server algorithm encryption show command.

```
> ssh server algorithm encryption show
+-------------- SSH SERVER ENCRYPTION ALGORITHM CONFIGURATION -------------+
| Algorithm Name                       | Priority | Admin State | Oper State|
+-------------------------------------+----------+-------------+-----------+
| aes128-ctr                           | 1        | Enabled     | Enabled   |
| aes192-ctr                           | 2        | Enabled     | Enabled   |
| aes256-ctr                           | 3        | Enabled     | Enabled   |
| arcfour256                           | 4        | Enabled     | Disabled  |
| arcfour128                           | 5        | Enabled     | Disabled  |
| aes128-gcm@openssh.com               | 6        | Enabled     | Disabled  |
| aes256-gcm@openssh.com               | 7        | Enabled     | Disabled  |
| chacha20-poly1305@openssh.com        | 8        | Enabled     | Disabled  |
| aes128-cbc                           | 9        | Enabled     | Enabled   |
| 3des-cbc                             | 10       | Enabled     | Enabled   |
| blowfish-bc                          | 11       | Enabled     | Disabled  |
| cast128-                             | 12       | Enabled     | Disabled  |
| aes192-cbc                           | 13       | Enabled     | Enabled   |
| aes256-cbc                           | 14       | Enabled     | Enabled   |
| arcfour                              | 15       | Enabled     | Disabled  |
| rijndael-cbc@lysator.liu.se          | 16       | Enabled     | Enabled   |
+-------------------------------------+----------+-------------+-----------+
```

Procedure 10-7
Displaying SSH server algorithm configurations

You can display specific SSH server algorithm configurations and all SSH server algorithm configurations.

Step	Action

To display the SSH server encryption algorithm

1 Display the SSH server encryption algorithm configuration and states:

```
ssh server algorithm encryption show
```

To display the SSH server public-key-authentication algorithm

2 Display the SSH server public key authentication algorithm configuration and states:

```
ssh server algorithm public-key-authentication show
```

To display the SSH server key exchange algorithm

3 Display the SSH client key exchange algorithm:

```
ssh server algorithm kex show
```

To display the SSH server MAC algorithm

4 Display the SSH client MAC algorithm:

```
ssh client algorithm mac show
```

To display the all SSH server algorithms

5 Display a summary of all SSH server algorithm configurations and states:

```
ssh server algorithm show
```

—end—

Examples

This example shows the output for the ssh client algorithm encryption show command.

```
> ssh client algorithm encryption show
```

This example shows the output from the ssh server algorithm public-key-authentication show command.

```
> ssh server algorithm public-key-authentication show
```

```
+-------- SSH SERVER PUBLIC-KEY-AUTHENTICATION ALGORITHM CONFIGURATION --------+
| Algorithm Name                                    | Admin State | Oper State |
+---------------------------------------------------+-------------+------------+
| ssh-dss                                           | Enabled     | Enabled    |
| ssh-rsa                                           | Enabled     | Enabled    |
| ssh-ed25519                                       | Enabled     | Enabled    |
| ecdsa-sha2-nistp256                               | Enabled     | Enabled    |
| ecdsa-sha2-nistp384                               | Enabled     | Enabled    |
| ecdsa-sha2-nistp521                               | Enabled     | Enabled    |
+---------------------------------------------------+-------------+------------+
```

This example shows the output from the ssh server algorithm kex show command.

```
> ssh server algorithm kex show

+------------------- SSH SERVER KEX ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| curve25519-sha256@libssh.org           | 1        | Enabled     | Enabled    |
| ecdh-sha2-nistp256                     | 2        | Enabled     | Enabled    |
| ecdh-sha2-nistp384                     | 3        | Enabled     | Enabled    |
| ecdh-sha2-nistp521                     | 4        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256   | 5        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1     | 6        | Enabled     | Enabled    |
| diffie-hellman-group14-sha1            | 7        | Enabled     | Enabled    |
| diffie-hellman-group1-sha1             | 8        | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
```

This shows the output for the ssh server algorithm show command.

```
> ssh server algorithm show

+------------------- SSH SERVER KEX ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| curve25519-sha256@libssh.org           | 1        | Enabled     | Enabled    |
| ecdh-sha2-nistp256                     | 2        | Enabled     | Enabled    |
| ecdh-sha2-nistp384                     | 3        | Enabled     | Enabled    |
| ecdh-sha2-nistp521                     | 4        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256   | 5        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1     | 6        | Enabled     | Enabled    |
| diffie-hellman-group14-sha1            | 7        | Enabled     | Enabled    |
| diffie-hellman-group1-sha1             | 8        | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+

+--------------- SSH SERVER ENCRYPTION ALGORITHM CONFIGURATION ----------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| aes128-ctr                             | 1        | Enabled     | Enabled    |
| aes192-ctr                             | 2        | Enabled     | Enabled    |
| aes256-ctr                             | 3        | Enabled     | Enabled    |
| arcfour256                             | 4        | Enabled     | Enabled    |
| arcfour128                             | 5        | Enabled     | Enabled    |
| aes128-gcm@openssh.com                 | 6        | Enabled     | Enabled    |
| aes256-gcm@openssh.com                 | 7        | Enabled     | Enabled    |
| chacha20-poly1305@openssh.com          | 8        | Enabled     | Enabled    |
| aes128-cbc                             | 9        | Enabled     | Enabled    |
| 3des-cbc                               | 10       | Enabled     | Enabled    |
| blowfish-cbc                           | 11       | Enabled     | Enabled    |
| cast128-cbc                            | 12       | Enabled     | Enabled    |
| aes192-cbc                             | 13       | Enabled     | Enabled    |
| aes256-cbc                             | 14       | Enabled     | Enabled    |
| arcfour                                | 15       | Enabled     | Enabled    |
| rijndael-cbc@lysator.liu.se            | 16       | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
+------------------- SSH SERVER MAC ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                          | Priority | Admin State | Oper State |
+-----------------------------------------+----------+-------------+------------+
| hmac-md5-etm@openssh.com                | 1        | Enabled     | Enabled    |
| hmac-sha1-etm@openssh.com               | 2        | Enabled     | Enabled    |
| umac-64-etm@openssh.com                 | 3        | Enabled     | Enabled    |
| umac-128-etm@openssh.com                | 4        | Enabled     | Enabled    |
| hmac-sha2-256-etm@openssh.com           | 5        | Enabled     | Enabled    |
| hmac-sha2-512-etm@openssh.com           | 6        | Enabled     | Enabled    |
| hmac-ripemd160-etm@openssh.com          | 7        | Enabled     | Enabled    |
| hmac-sha1-96-etm@openssh.com            | 8        | Enabled     | Enabled    |
| hmac-md5-96-etm@openssh.com             | 9        | Enabled     | Enabled    |
| hmac-md5                                | 10       | Enabled     | Enabled    |
| hmac-sha1                               | 11       | Enabled     | Enabled    |
| umac-64@openssh.com                     | 12       | Enabled     | Enabled    |
| umac-128@openssh.com                    | 13       | Enabled     | Enabled    |
| hmac-sha2-256                           | 14       | Enabled     | Enabled    |
| hmac-sha2-512                           | 15       | Enabled     | Enabled    |
| hmac-ripemd160                          | 16       | Enabled     | Enabled    |
| hmac-ripemd160@openssh.com              | 17       | Enabled     | Enabled    |
| hmac-sha1-96                            | 18       | Enabled     | Enabled    |
| hmac-md5-96                             | 19       | Enabled     | Enabled    |
+-----------------------------------------+----------+-------------+------------+

+-------- SSH SERVER PUBLIC-KEY-AUTHENTICATION ALGORITHM CONFIGURATION --------+
| Algorithm Name                                     | Admin State | Oper State |
+----------------------------------------------------+-------------+------------+
| ssh-dss                                            | Enabled     | Enabled    |
| ssh-rsa                                            | Enabled     | Enabled    |
| ssh-ed25519                                        | Enabled     | Enabled    |
| ecdsa-sha2-nistp256                                | Enabled     | Enabled    |
| ecdsa-sha2-nistp384                                | Enabled     | Enabled    |
| ecdsa-sha2-nistp521                                | Enabled     | Enabled    |
+----------------------------------------------------+-------------+------------+
```

Procedure 10-8
Configuring the SSH server priority of an encryption algorithm

You can configure the SSH server priority of an encryption algorithm. The highest priority is 1. This setting causes other algorithm priorities to adjust accordingly.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Configure the SSH server priority of a specified encryption algorithm:

```
ssh server algorithm encryption set algorithm
<encryption-algorithm> priority <NUMBER: 1..16>
```

where

encryption-algorithm	is the specific algorithm.
priority <NUMBER: 1..16>	sets the priority of the specified algorithm.

—end—

Example

This example shows the output from the ssh server algorithm encryption set algorithm ? command

```
> ssh server algorithm encryption set algorithm ?

encryption algorithm
Possible SshServerEncryptionAlgorithm values:
    3des-cbc                           aes256-gcm@openssh.com
    aes128-cbc                         arcfour
    aes128-ctr                         arcfour128
    aes128-gcm@openssh.com             arcfour256
    aes192-cbc                         blowfish-cbc
    aes192-ctr                         cast128-cbc
    aes256-cbc                         chacha20-poly1305@openssh.com
    aes256-ctr                         rijndael-cbc@lysator.liu.se
^C                            Kill Command Composition/Execution/Displayssh
>server algorithm encryption set algorithm 3des-cbc priority 1
```

Procedure 10-9
Configuring the SSH server priority of a key exchange algorithm

Configure the SSH server priority of a key exchange algorithm. The highest priority is 1. This setting causes other algorithm priorities to adjust accordingly.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Configure the SSH server priority of a key exchange algorithm:

```
ssh server algorithm kex set algorithm <kex-algorithm>
priority <NUMBER: 1..8>
```

where

kex-algorithm	is the key exchange algorithm.
priority <NUMBER: 1..8>	sets the priority of the specified algorithm.

—end—

Example

This example configures the SSH server priority of a key exchange algorithm.

```
> ssh server algorithm kex show

>+---------------- SSH SERVER KEX ALGORITHM CONFIGURATION -----------------+
| Algorithm Name                       |Priority| Admin State | Oper State |
+--------------------------------------+--------+-------------+------------+
| curve25519-sha256@libssh.org         | 1      | Enabled     | Enabled    |
| ecdh-sha2-nistp256                   | 2      | Enabled     | Enabled    |
| ecdh-sha2-nistp384                   | 3      | Enabled     | Enabled    |
| ecdh-sha2-nistp521                   | 4      | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256 | 5      | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1   | 6      | Enabled     | Enabled    |
| diffie-hellman-group14-sha1          | 7      | Enabled     | Enabled    |
| diffie-hellman-group1-sha1           | 8      | Enabled     | Enabled    |
+--------------------------------------+---------+-------------+-----------+

>ssh server algorithm kex set algorithm ecdh-sha2-nistp521 priority 2

> ssh server algorithm kex show
>+---------------- SSH SERVER KEX ALGORITHM CONFIGURATION -----------------+
| Algorithm Name                       |Priority| Admin State | Oper State |
+--------------------------------------+--------+-------------+------------+
| curve25519-sha256@libssh.org         | 1      | Enabled     | Enabled    |
| ecdh-sha2-nistp521                   | 2      | Enabled     | Enabled    |
| ecdh-sha2-nistp256                   | 3      | Enabled     | Enabled    |
| ecdh-sha2-nistp384                   | 4      | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256 | 5      | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1   | 6      | Enabled     | Enabled    |
| diffie-hellman-group14-sha1          | 7      | Enabled     | Enabled    |
| diffie-hellman-group1-sha1           | 8      | Enabled     | Enabled    |
+--------------------------------------+--------+-------------+------------+
```

Procedure 10-10
Configuring the SSH server priority of a MAC algorithm

Configure the SSH server priority of a MAC algorithm. The highest priority is 1. This setting causes other algorithm priorities to adjust accordingly.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Configure the SSH server priority of a MAC algorithm:

```
ssh server algorithm mac set algorithm <mac-algorithm>
priority <NUMBER: 1..19>
```

where

mac-algorithm	is the key exchange algorithm.
priority <NUMBER: 1..19>	sets the priority of the specified algorithm.

—end—

Example

This example configures the SSH server priority of a MAC algorithm.

```
> ssh server algorithm mac show

+------------------ SSH SERVER MAC ALGORITHM CONFIGURATION ----------------+
| Algorithm Name                     | Priority | Admin State | Oper State |
+------------------------------------+----------+-------------+------------+
| hmac-md5-etm@openssh.com           | 1        | Enabled     | Disabled   |
| hmac-sha1-etm@openssh.com          | 2        | Enabled     | Disabled   |
| umac-64-etm@openssh.com            | 3        | Enabled     | Disabled   |
| umac-128-etm@openssh.com           | 4        | Enabled     | Disabled   |
| hmac-sha2-256-etm@openssh.com      | 5        | Enabled     | Disabled   |
| hmac-sha2-512-etm@openssh.com      | 6        | Enabled     | Disabled   |
| hmac-ripemd160-etm@openssh.com     | 7        | Enabled     | Disabled   |
| hmac-sha1-96-etm@openssh.com       | 8        | Enabled     | Disabled   |
| hmac-md5-96-etm@openssh.com        | 9        | Enabled     | Disabled   |
| hmac-md5                           | 10       | Enabled     | Disabled   |
| hmac-sha1                          | 11       | Enabled     | Enabled    |
| umac-64@openssh.com                | 12       | Enabled     | Disabled   |
| umac-128@openssh.com               | 13       | Enabled     | Disabled   |
| hmac-sha2-256                      | 14       | Enabled     | Enabled    |
| hmac-sha2-512                      | 15       | Enabled     | Enabled    |
| hmac-ripemd160                     | 16       | Enabled     | Disabled   |
| hmac-ripemd160@openssh.com         | 17       | Enabled     | Disabled   |
| hmac-sha1-96                       | 18       | Enabled     | Disabled   |
| hmac-md5-96                        | 19       | Enabled     | Disabled   |
+------------------------------------+----------+-------------+------------+
>ssh server algorithm mac set algorithm ecdh-sha2-nistp256 priority 12
```

Procedure 10-11
Enabling and disabling an encryption algorithm on the SSH client

Enable or disable an encryption algorithm on the SSH client according to the network operator security plan. You must have administrative user privileges to perform this procedure.

Step **Action**

1 Enable or disable an encryption algorithm on the SSH client:

```
ssh client algorithm encryption <enable|disable>
algorithm <encryption-algorithm>
```

where

enable|disable enables the encryption algorithm

encryption-algorithm is the specific algorithm.

kex-algorithm enables or disables the key exchange algorithm.

—end—

Example

This example enables an encryption algorithm on the SSH client.

```
> ssh client algorithm encryption show

+------------- SSH CLIENT ENCRYPTION ALGORITHM CONFIGURATION --------------+
| Algorithm Name                     | Priority | Admin State | Oper State |
+------------------------------------+----------+-------------+------------+
| aes128-ctr                         | 1        | Enabled     | Enabled    |
| aes192-ctr                         | 2        | Enabled     | Enabled    |
| aes256-ctr                         | 3        | Enabled     | Enabled    |
| arcfour256                         | 4        | Enabled     | Disabled   |
| arcfour128                         | 5        | Enabled     | Disabled   |
| aes128-gcm@openssh.com             | 6        | Enabled     | Disabled   |
| aes256-gcm@openssh.com             | 7        | Enabled     | Disabled   |
| chacha20-poly1305@openssh.com      | 8        | Enabled     | Disabled   |
| aes128-cbc                         | 9        | Enabled     | Enabled    |
| 3des-cbc                           | 10       | Enabled     | Enabled    |
| blowfish-cbc                       | 11       | Enabled     | Disabled   |
| cast128-cbc                        | 12       | Enabled     | Disabled   |
| aes192-cbc                         | 13       | Enabled     | Enabled    |
| aes256-cbc                         | 14       | Enabled     | Enabled    |
| arcfour                            | 15       | Enabled     | Disabled   |
| rijndael-cbc@lysator.liu.se        | 16       | Enabled     | Enabled    |
+-------------------------------------+----------+-------------+-----------+
>ssh client algorithm encryption enable algorithm aes128-ctr
```

Procedure 10-12
Configuring the SSH client priority of an encryption algorithm

You can configure the SSH client priority of a specified encryption algorithm. The highest priority is 1. This setting causes other algorithm priorities to adjust accordingly.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Configure the SSH server priority of a specified encryption algorithm:

```
ssh client algorithm encryption set algorithm
<encryption-algorithm> priority <NUMBER: 1..16>
```

where

encryption-algorithm is the specific algorithm.

priority <NUMBER: 1..16> sets the priority of the specified algorithm.

—end—

Example

This example configures the SSH client priority of an encryption algorithm.

```
> ssh client algorithm encryption show

+------------- SSH CLIENT ENCRYPTION ALGORITHM CONFIGURATION --------------+
| Algorithm Name                     | Priority | Admin State | Oper State |
+------------------------------------+----------+-------------+------------+
| aes128-ctr                         | 1        | Enabled     | Enabled    |
| aes192-ctr                         | 2        | Enabled     | Enabled    |
| aes256-ctr                         | 3        | Enabled     | Enabled    |
| arcfour256                         | 4        | Enabled     | Disabled   |
| arcfour128                         | 5        | Enabled     | Disabled   |
| aes128-gcm@openssh.com             | 6        | Enabled     | Disabled   |
| aes256-gcm@openssh.com             | 7        | Enabled     | Disabled   |
| chacha20-poly1305@openssh.com      | 8        | Enabled     | Disabled   |
| aes128-cbc                         | 9        | Enabled     | Enabled    |
| 3des-cbc                           | 10       | Enabled     | Enabled    |
| blowfish-cbc                       | 11       | Enabled     | Disabled   |
| cast128-cbc                        | 12       | Enabled     | Disabled   |
| aes192-cbc                         | 13       | Enabled     | Enabled    |
| aes256-cbc                         | 14       | Enabled     | Enabled    |
| arcfour                            | 15       | Enabled     | Disabled   |
| rijndael-cbc@lysator.liu.se        | 16       | Enabled     | Enabled    |
+------------------------------------+----------+-------------+------------+
>ssh client algorithm encryption set algorithm aes128-ctr priority 12
```

Procedure 10-13
Configuring the SSH client priority of a key exchange algorithm

Configure the SSH client priority of a key exchange algorithm according to the network operator security plan. The highest priority is 1. This setting causes other algorithm priorities to adjust accordingly.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Configure the SSH client priority of a key exchange algorithm:

```
ssh client algorithm kex set algorithm <kex-algorithm>
priority <NUMBER: 1..8>
```

where

kex-algorithm	is the key exchange algorithm.
priority <NUMBER: 1..8>	sets the priority of the specified algorithm.

—end—

Example

This example configures the SSH client priority of an key exchange algorithm.

```
> ssh client algorithm kex show

+------------------ SSH CLIENT KEX ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                        |Priority| Admin State | Oper State |
+--------------------------------------+----------+-------------+-----------+
| curve25519-sha256@libssh.org          | 1        | Enabled      | Enabled    |
| ecdh-sha2-nistp256                    | 2        | Enabled      | Enabled    |
| ecdh-sha2-nistp384                    | 3        | Enabled      | Enabled    |
| ecdh-sha2-nistp521                    | 4        | Enabled      | Enabled    |
| diffie-hellman-group-exchange-sha256  | 5        | Enabled      | Enabled    |
| diffie-hellman-group-exchange-sha1    | 6        | Enabled      | Enabled    |
| diffie-hellman-group14-sha1           | 7        | Enabled      | Enabled    |
| diffie-hellman-group1-sha1            | 8        | Enabled      | Enabled    |
+---------------------------------------+--------+-------------+-----------+
>ssh client algorithm kex set algorithm ecdh-sha2-nistp256 priority 2
```

Procedure 10-14
Displaying SSH client algorithm configurations

You can display specific SSH client algorithm configurations and all SSH client algorithm configurations.

Step **Action**

To display the SSH client encryption algorithm

1 Display a summary of SSH client encryption algorithm configuration and states:

```
ssh client algorithm encryption show
```

To display the SSH client key exchange algorithm

2 Display the SSH client key exchange algorithm:

```
ssh client algorithm kex show
```

To display the SSH client MAC algorithm

3 Display the SSH client MAC algorithm:

```
ssh client algorithm mac show
```

To display the all SSH client algorithms

4 Display a summary of all SSH client algorithm configurations and states:

```
ssh client algorithm show
```

—end—

Examples

This example shows the output for the ssh client algorithm encryption show command.

```
> ssh client algorithm encryption show

+--------------- SSH CLIENT ENCRYPTION ALGORITHM CONFIGURATION -----------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| aes128-ctr                             | 1        | Enabled     | Enabled    |
| aes192-ctr                             | 2        | Enabled     | Enabled    |
| aes256-ctr                             | 3        | Enabled     | Enabled    |
| arcfour256                             | 4        | Enabled     | Enabled    |
| arcfour128                             | 5        | Enabled     | Enabled    |
| aes128-gcm@openssh.com                 | 6        | Enabled     | Enabled    |
| aes256-gcm@openssh.com                 | 7        | Enabled     | Enabled    |
| chacha20-poly1305@openssh.com          | 8        | Enabled     | Enabled    |
| aes128-cbc                             | 9        | Enabled     | Enabled    |
| 3des-cbc                               | 10       | Enabled     | Enabled    |
| blowfish-cbc                           | 11       | Enabled     | Enabled    |
| cast128-cbc                            | 12       | Enabled     | Enabled    |
| aes192-cbc                             | 13       | Enabled     | Enabled    |
| aes256-cbc                             | 14       | Enabled     | Enabled    |
| arcfour                                | 15       | Enabled     | Enabled    |
| rijndael-cbc@lysator.liu.se            | 16       | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
```

This example shows the output for the ssh client kex show command.

```
> ssh client algorithm kex show

+------------------- SSH CLIENT KEX ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| curve25519-sha256@libssh.org           | 1        | Enabled     | Enabled    |
| ecdh-sha2-nistp256                     | 2        | Enabled     | Enabled    |
| ecdh-sha2-nistp384                     | 3        | Enabled     | Enabled    |
| ecdh-sha2-nistp521                     | 4        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256   | 5        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1     | 6        | Enabled     | Enabled    |
| diffie-hellman-group14-sha1            | 7        | Enabled     | Enabled    |
| diffie-hellman-group1-sha1             | 8        | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
```

This example shows the output for the ssh client algorithm mac show command.

```
> ssh client algorithm mac show

+------------------- SSH CLIENT MAC ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| hmac-md5-etm@openssh.com               | 1        | Enabled     | Enabled    |
| hmac-sha1-etm@openssh.com              | 2        | Enabled     | Enabled    |
| umac-64-etm@openssh.com                | 3        | Enabled     | Enabled    |
| umac-128-etm@openssh.com               | 4        | Enabled     | Enabled    |
| hmac-sha2-256-etm@openssh.com          | 5        | Enabled     | Enabled    |
| hmac-sha2-512-etm@openssh.com          | 6        | Enabled     | Enabled    |
| hmac-ripemd160-etm@openssh.com         | 7        | Enabled     | Enabled    |
| hmac-sha1-96-etm@openssh.com           | 8        | Enabled     | Enabled    |
| hmac-md5-96-etm@openssh.com            | 9        | Enabled     | Enabled    |
| hmac-md5                               | 10       | Enabled     | Enabled    |
| hmac-sha1                              | 11       | Enabled     | Enabled    |
| umac-64@openssh.com                    | 12       | Enabled     | Enabled    |
| umac-128@openssh.com                   | 13       | Enabled     | Enabled    |
| hmac-sha2-256                          | 14       | Enabled     | Enabled    |
| hmac-sha2-512                          | 15       | Enabled     | Enabled    |
| hmac-ripemd160                         | 16       | Enabled     | Enabled    |
| hmac-ripemd160@openssh.com             | 17       | Enabled     | Enabled    |
| hmac-sha1-96                           | 18       | Enabled     | Enabled    |
| hmac-md5-96                            | 19       | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
```

This example shows the output for the ssh client algorithm show command.

```
> ssh client algorithm show

+------------------- SSH CLIENT KEX ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| curve25519-sha256@libssh.org           | 1        | Enabled     | Enabled    |
| ecdh-sha2-nistp256                     | 2        | Enabled     | Enabled    |
| ecdh-sha2-nistp384                     | 3        | Enabled     | Enabled    |
| ecdh-sha2-nistp521                     | 4        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha256   | 5        | Enabled     | Enabled    |
| diffie-hellman-group-exchange-sha1     | 6        | Enabled     | Enabled    |
| diffie-hellman-group14-sha1            | 7        | Enabled     | Enabled    |
| diffie-hellman-group1-sha1             | 8        | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+

+--------------- SSH CLIENT ENCRYPTION ALGORITHM CONFIGURATION ----------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| aes128-ctr                             | 1        | Enabled     | Enabled    |
| aes192-ctr                             | 2        | Enabled     | Enabled    |
| aes256-ctr                             | 3        | Enabled     | Enabled    |
| arcfour256                             | 4        | Enabled     | Enabled    |
| arcfour128                             | 5        | Enabled     | Enabled    |
| aes128-gcm@openssh.com                 | 6        | Enabled     | Enabled    |
| aes256-gcm@openssh.com                 | 7        | Enabled     | Enabled    |
| chacha20-poly1305@openssh.com          | 8        | Enabled     | Enabled    |
| aes128-cbc                             | 9        | Enabled     | Enabled    |
| 3des-cbc                               | 10       | Enabled     | Enabled    |
| blowfish-cbc                           | 11       | Enabled     | Enabled    |
| cast128-cbc                            | 12       | Enabled     | Enabled    |
| aes192-cbc                             | 13       | Enabled     | Enabled    |
| aes256-cbc                             | 14       | Enabled     | Enabled    |
| arcfour                                | 15       | Enabled     | Enabled    |
| rijndael-cbc@lysator.liu.se            | 16       | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+

+------------------- SSH CLIENT MAC ALGORITHM CONFIGURATION -------------------+
| Algorithm Name                         | Priority | Admin State | Oper State |
+----------------------------------------+----------+-------------+------------+
| hmac-md5-etm@openssh.com               | 1        | Enabled     | Enabled    |
| hmac-sha1-etm@openssh.com              | 2        | Enabled     | Enabled    |
| umac-64-etm@openssh.com                | 3        | Enabled     | Enabled    |
| umac-128-etm@openssh.com               | 4        | Enabled     | Enabled    |
| hmac-sha2-256-etm@openssh.com          | 5        | Enabled     | Enabled    |
| hmac-sha2-512-etm@openssh.com          | 6        | Enabled     | Enabled    |
| hmac-ripemd160-etm@openssh.com         | 7        | Enabled     | Enabled    |
| hmac-sha1-96-etm@openssh.com           | 8        | Enabled     | Enabled    |
| hmac-md5-96-etm@openssh.com            | 9        | Enabled     | Enabled    |
| hmac-md5                               | 10       | Enabled     | Enabled    |
| hmac-sha1                              | 11       | Enabled     | Enabled    |
| umac-64@openssh.com                    | 12       | Enabled     | Enabled    |
| umac-128@openssh.com                   | 13       | Enabled     | Enabled    |
| hmac-sha2-256                          | 14       | Enabled     | Enabled    |
| hmac-sha2-512                          | 15       | Enabled     | Enabled    |
| hmac-ripemd160                         | 16       | Enabled     | Enabled    |
| hmac-ripemd160@openssh.com             | 17       | Enabled     | Enabled    |
| hmac-sha1-96                           | 18       | Enabled     | Enabled    |
| hmac-md5-96                            | 19       | Enabled     | Enabled    |
+----------------------------------------+----------+-------------+------------+
```

Procedure 10-15
Configuring SSH client certificates

Configure SSH client certificates according to the network operator security plan.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Create client certificate:

```
ssh client certificate csr generate user <String[1..32]>
```

2 Install certificate:

```
ssh client certificate install user <String[1..32]>
```

3 Display client certificate:

```
ssh client certificate show
```

—end—

Procedure 10-16
Configuring new host keys for SSH client connection

Configure new host keys for SSH client certificates according to the network operator security plan.

When the SFTP server is validated, the 8700 switch attempts to connect to the specified server and validates the host key provided by the server against the system known hosts file. If the key does not match it is an error. If there is no key for the server the user is interactively presented with the servers host key and allowed to add or reject the key.

You must have super user privileges to perform this procedure.

Step **Action**

1 Remove IP/Host's key from the system managed known hosts file:

```
ssh client system-client remove ip <ip-host-str>
```

2 Enable host-key check:

```
ssh client system-client <ignore|non-strict|strict>
```

where

ignore	disables host-key checking for SSH client connections initiated by the SAOS system
non-strict	SSH client connections initiated (new host keys automatically accepted, changed host keys rejected)
strict	enables strict non-interactive host-key checking for SSH client connections initiated by the SAOS system. (new keys or changed host-keys rejected)

3 Validate SFTP server:

```
ssh client system-client validate sftp-server <ipaddress>
login-id <user> [server-port <port>]
```

4 Display SSH client system-client attributes:

```
ssh client system-client show>
```

—end—

Procedure 10-17
Configuring peer certificate re-authentication for SSH clients

Configure peer certificate re-authentication for SSH clients according to the network operator security plan.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Enable SSH client peer re-authentication:

```
ssh client peer-cert-reauth enable
```

2 Set the re-authentication period

```
ssh client peer-cert-reauth set {[period
<duration>][ocsp-multiplier <NUMBER: 0..50>]}
```

where

period duration	Sets the re-authentication period. The default is 1 hr).
ocsp-multiplier	defines the period between doing OCSP when re-authenticating (OCSP period = re-authentication period * ocsp-multiplier.) The default is 24hr.

3 Display peer certificate re-authentication attributes:

```
ssh client peer-cert-reauth show
```

—end—

Procedure 10-18
Configuring peer certificate re-authentication for SSH servers

Configure new host keys for SSH server certificates according to the network operator security plan.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Enable SSH server peer re-authentication:

```
ssh server peer-cert-reauth enable
```

2 Set the re-authentication period

```
ssh server peer-cert-reauth set {[period
<duration>][ocsp-multiplier <NUMBER: 0..50>]}
```

where

period duration	Sets the re-authentication period. The default is 1 hr).
ocsp-multiplier	defines the period between doing OCSP when re-authenticating (OCSP period = re-authentication period * ocsp-multiplier.) The default is 24hr.

3 Display server certificate re-authentication attributes:

```
ssh server peer-cert-reauth show
```

—end—

Procedure 10-19
Connecting to an SSH client

Use SSH to connect to a client using the IP address or host name.

Step	**Action**
1	Connect to an SSH client using the IP address or host name in one of these ways:

```
ssh client connect ip <IP address or host name>
```

where

ip <IP address or host name>	is the IP address or host name.

—end—

Procedure 10-20
Copying files by means of secure copy

Copy files by means of secure copy in a source or destination mode.

You can copy a file

- to a remote location
- from a remote location
- from a remote location to another remote location

Step **Action**

To copy a file to a remote location

1 Copy a file to a remote location:

```
file scp/tmp/<filename> remote@REMOTE_HOST:<filename>
```

To copy a file from a remote location

2 Copy a file from a remote location:

```
file scp remote@REMOTE_HOST:<filename>/tmp/<filename>
```

To copy a file from a remote location to another remote location

3 Copy a file from a remote location to another remote location:

```
file scp remote@REMOTE_HOST:/<filename>
remote2@REMOTE_HOST_TWO:<filename>
```

—end—

Example

This example copies a file to a remote location:

```
> file scp/ tmp/file0 remote@REMOTE_HOST:file0
```

This example copies a file from a remote location:

```
> file scp remote@REMOTE_HOST:file0 /tmp/file0
```

This example copies a file from a remote location to another remote location:

```
> file scp remote@remote_HOST:/file0 remote2@REMOTE_host_two:/file0
```

Procedure 10-21
Enabling and disabling the SFTP server

The SFTP server is disabled by default.

> **CAUTION**
> **Traffic disruption risk**
> Although you can enable the SFTP server, doing so creates a security hole that allows a malicious user potentially harmful access to the Linux shell.

Ciena recommends that the SFTP server remain disabled.

Step **Action**

To enable the SFTP server

1 Enable the SFTP server:

```
system server sftp enable
```

The system displays this warning:

```
WARNING: Turning this on will reduce the security of this
installation!

Contact Ciena Support for more information.
```

To disable the SFTP server

2 Disable the SFTP server:

```
system server sftp disable
```

To display the state of the SFTP server

3 Enter this command to display the SFTP server setting:

```
system server sftp show
```

The system responds with the status similar to the following:

```
+-------- SFTP SERVER --------+
| State | Disabled            |
+-------+---------------------+
```

—end—

Procedure 10-22
Configuring the SSH/SFTP Client

Configure the SSH-SFTP client according to network requirements. Client keys can be generated on the SAOS switch from an external source.

You can configure:

- a default remote SFTP server
- SSH/SFTP Client for X.509 Host Key Authentication using the 8700 switch
- SSH/SFTP Client for X.509 Host Key Authentication using an external source
- install the CA certificate to validate incoming x509 certificates
- install the signed certificate on an SAOS switch for the client

Step	Action

To configure a default remote SFTP server

1 Configure the default remote SFTP server:

```
system xftp set sftp-server <ipaddress> login-id <string>
echoless-password <string>
```

To configure SSH/SFTP Client for X.509 Host Key Authentication using the SAOS switch

2 Generate the client private key:

```
ssh client key generate user <user> [force] [key-type]
```

3 -Create the client X.509 certificate from the private key and an off-the box config file:

```
ssh client certificate csr generate user <user> filename
<ca-certificate> xftp-server <ipaddress> login-id <xftp
user> echoless-password
```

To configure SSH/SFTP Client for X.509 Host Key Authentication using an external source

4 Create the client X.509 certificate from an off-the-box private key and config file:

```
ssh client key install user <user> filename <ca-
certificate> xftp-server <ipaddress> login-id <xftp user>
echoless-password
```

To install the CA certificate to validate incoming x509 certificates

5 Install the CA certificate to validate incoming x509 certificates:

```
system security pkix ca install filename <ca-certificate>
xftp-server <ipaddress> login-id <xftp user> echoless-
password
```

To install the signed certificate on an SAOS switch for the client

6 Install the signed certificate on an SAOS switch for the client:

```
ssh client certificate install user <user> ftp-server
<ipaddress> filename <user-certificate> login-id <xftp
user> echoless-password
```

—end—

Example

In the following examples, “admin17” configures an SSH client for user “super1” using an x.509 certificate. After the certificate is installed, client algorithm priorities can be changed or disabled as needed.

This example generates a private key on the SAOS switch, uses the key and an SFTP server config file to generate the certificate, installs the certificate on the SFTP server, then installs the certificate on the SAOS switch:

```
> ssh client key generate user super1 key-type rsa2048
> ssh client certificate csr generate user super1 filename /var/lib/tftpboot/
sshTest1/ClientCA/RadSecDevCert.cnf sftp-server xx.xxx.xxx.xx login-id
admin17 echoless-password
> system security pkix ca install sftp-server xx.xxx.xxx.xx filename /var/lib/
tftpboot/sshTest1/ServerCA/RadSecSrvCA.pem login-id admin17 echoless-
password
> ssh client certificate install user super1 sftp-server xx.xxx.xxx.xx
filename /var/lib/tftpboot/sshTest1/ClientCA/RadSecDevCert.pem login-id
admin17 echoless-password echoless-passphrase
> ssh client algorithm host-key-authentication set algorithm x509v3-sign-rsa
priority 1
> ssh client algorithm host-key-authentication disable algorithm ssh-rsa
> ssh client algorithm host-key-authentication disable algorithm ssh-dss
> ssh client algorithm host-key-authentication disable algorithm ssh-ed25519
> ssh client algorithm host-key-authentication disable algorithm rsa-sha2-256
> ssh client algorithm host-key-authentication disable algorithm rsa-sha2-512
> ssh client connect ip xx.xxx.xxx.xx user super1
```

This example installs a private key from an SFTP server, installs the certificate on the SFTP server, then installs the certificate on the SAOS switch:

```
> ssh client key install user super1 filename /var/lib/tftpboot/sshTest1/
ClientCA/RadSecDevCert.csr sftp-server xx.xxx.xxx.xx login-id admin17
echoless-password
> system security pkix ca install sftp-server xx.xxx.xxx.xx filename /var/lib/
tftpboot/sshTest1/ServerCA/RadSecSrvCA.pem login-id admin17 echoless-
password
> ssh client certificate install user super1 sftp-server xx.xxx.xxx.xx
filename /var/lib/tftpboot/sshTest1/ClientCA/RadSecDevCert.pem login-id
admin17 echoless-password echoless-passphrase
> ssh client algorithm host-key-authentication set algorithm x509v3-sign-rsa
priority 1
> ssh client algorithm host-key-authentication disable algorithm ssh-rsa
> ssh client algorithm host-key-authentication disable algorithm ssh-dss
> ssh client algorithm host-key-authentication disable algorithm ssh-ed25519
> ssh client algorithm host-key-authentication disable algorithm rsa-sha2-256
> ssh client algorithm host-key-authentication disable algorithm rsa-sha2-512
> ssh client connect ip xx.xxx.xxx.xx user super1
```

Procedure 10-23
Transferring files with the SFTP client

Transfer files with the SFTP client when

- customer support directs you to transfer a file from the switch
- when you want to make a backup copy of a configuration file

Step **Action**

1 Configure the system for SFTP:

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

where

sftp-server <ip-host-str>	is the SFTP server. The SFTP server supports both IPv4 and IPv6 clients.
login-id <username>	is the sftp username.
password-attr	is the echoless-password.
echoless-password-attr	collects the password interactively.
server-port <INTEGER: 1...65535>	is the server-port number to connect to

To get a file from an SFP server

2 Get a file from an SFTP server:

```
system xftp getfile {sftp-server <ip-host-str> login-id
<username> {<password-attr>|<echoless-password-
attr>}[<remote-filename>] [<local-filename>] [server-
port <INTEGER: 1...65535>]}}
```

To put a file on an SFP server

3 Put a file to an SFTP server:

```
system xftp putfile {sftp-server <ip-host-str> login-id
<username> {<password-attr>|<echoless-password-
attr>}[<remote-filename>] [<local-filename>] [server-
port <INTEGER: 1...65535>]}}
```

—end—

Procedure 10-24
Transferring files with the FTP client

Transfer files with the FTP client when

- customer support directs you to transfer a file from the switch
- you want to make a backup copy of a configuration file

Step	Action

1 Configure the system for FTP:

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

where

ftp-server <ip-host-str>	is the ftp-server name.
login-id <username>	is the FTP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

To get a file from an FTP server

2 Get a file from an FTP server:

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

To put a file on an FTP server

3 Put a file to an FTP server:

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

—end—

Procedure 10-25
Transferring files with the TFTP client

Transfer files with the TFTP client when:

- customer support directs you to transfer a file
- you want to make a backup copy of a configuration file

Step **Action**

1 Configure the system for TFTP:

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

where

tftp-server <ip-host-str>	is the tftp-server name.
login-id <username>	is the TFTP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

To get a file from a TFTP server

2 Get a file from an TFTP server:

```
system xftp get file {tftp-server <ip-host-str> [login-id
<username> [<password-attr>|<echoless-password-
attr>][<remote-filename>] [<local-filename>] [server-
port <INTEGER: 1...65535>]}
```

To put a file from a TFTP server

3 Put a file to an TFTP server:

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

—end—

Procedure 10-26
Enabling or disabling the FTP or TFTP client

Supported FTP and TFTP client operations include:

- enable the FTP client or TFTP client
- disable the FTP client or TFTP client
- display the state of the FTP or TFTP server to determine whether it is enabled or disabled

Step Action

To enable the FTP client or TFTP client

1 Enable the FTP client or the TFTP client:

```
system xftp enable {ftp-client|tftp-client}
```

To disable the FTP client or TFTP client

2 Disable the FTP client or the TFTP client:

```
system xftp disable {ftp-client|tftp-client}
```

To display the state of the FTP or TFTP server on a device

3 Display the state of the FTP or TFTP server on a device:

```
system server tftp show
```

—end—

Procedure 10-27
Managing MAC tables

MAC table operations include:

- set the aging time
- set the mac-refresh
- enable aging
- disable aging
- display status and aging time

Step **Action**

To set the aging time and mac-refresh

1 Set the aging time and mac-refresh:

```
flow aging set {[time <Seconds: 10-1000000>][mac-refresh
<da-sa|sa>]}>
```

where

time <Seconds: 10-1000000>	is the number of seconds
mac-refresh<da-salsa	is the agemac based on SA or DA/SA refresh.

To enable aging

2 Enable aging:

```
flow aging enable
```

To disable aging

3 Disable aging:

```
flow aging disable
```

To display the status and aging time

4 Display the status and aging time:

```
flow aging show
```

—end—

Example

This example shows sample output for the flow aging show command.

```
> flow aging show
+---------- AGING-INFO ---------+
| Parameter       | Value       |
+-----------------+-------------+
| Status          | Enabled     |
| Time (Seconds)  | 300         |
| Mac Refresh     | da-sa       |
+-------------------------------+
```

Procedure 10-28
Enabling and disabling MAC learning control

With MAC learning control, you can disable or enable the learning of dynamic MAC entries for a specific VLAN or virtual switch. By default, MAC learning is enabled upon creation of a VLAN or virtual switch.

> ***Note:*** When you disable MAC learning on a VLAN or virtual switch, all the dynamically-learned entries associated with the VLAN or virtual switch are immediately flushed.

If a VLAN is currently attached to a virtual switch as its active VLAN, the configured MAC learning status of the VLAN is ignored and the operational MAC learning status is based on the configured status of the virtual switch.

MAC learning control operations include:

- enable MAC learning on a VLAN
- disable MAC learning on a VLAN
- enable MAC learning on a virtual switch
- disable MAC learning on a virtual switch

Step **Action**

To enable MAC learning on a VLAN

1 Enable MAC learning on a VLAN:

```
flow learning enable vlan <vlan>
```

where

vlan <vlan>	is the VLAN or list of VLANs to enable MAC learning on.

To disable MAC learning on a VLAN

2 Disable MAC learning on a VLAN:

```
flow learning disable vlan <vlan>
```

where

vlan <vlan>	is the VLAN or list of VLANs to disable MAC learning on.

To enable MAC learning on a virtual switch

3 Enable MAC learning on a virtual switch:

```
flow learning enable vs <vs>
```

where

vs <vs>	is the virtual switch to enable MAC learning on.

To disable MAC learning on a virtual switch

4 Disable MAC learning on a virtual switch:

```
flow learning disable vs <VirtualSwitch>
```

where

vs <vs>	is the virtual switch to disable MAC learning on.

—end—

Procedure 10-29
Displaying the status of MAC learning

Display the status of MAC learning.

Step **Action**

1 Display the status of MAC learning:

```
flow learning show [all | all-disabled-vlans | all-
disabled-vs | all-vlans | all-vs | vlan <vlan> | vs <vs>]
```

where

all displays the learning status of all VLANs and virtual switches.

all-disabled-vlans displays all VLANs with learning disabled.

all-disabled-vs displays all virtual switches with learning disabled.

all-vlans displays the learning status of all VLANs.

all-vs displays the learning status of all virtual switches.

vlan <vlan> is the VLAN or list of VLANs to display learning status for.

vs <vs> is the virtual switch to display learning status for.

—end—

Example

This example shows sample output for the flow learning show all command.

```
> flow learning show all

+------------------------ VLAN MAC LEARNING -------------------------+
| VLAN                                   | Learning Status           |
| ID   | Name                            | Admin       | Oper        |
+------+---------------------------------+-------------+-------------+
| 1    | Default                         | Enabled     | Enabled     |
| 14   | VLAN#14                         | Disabled    | Disabled    |
| 15   | VLAN#15                         | Enabled     | Enabled     |
| 101  | VLAN#101                        | Disabled    | VS Override |
| 102  | VLAN#102                        | Enabled     | VS Override |
| 127  | Mgmt                            | Enabled     | Enabled     |
| 201  | VLAN#201                        | Enabled     | Enabled     |
| 4001 | VLAN#4001                       | Enabled     | Enabled     |
| 4002 | VLAN#4002                       | Enabled     | Enabled     |
+------+---------------------------------+-------------+-------------+
+---------------- VS MAC LEARNING ----------------+
|                  | Active | Learning Status     |
| VS               | VLAN   | Admin    | Oper     |
+------------------+--------+----------+----------+
| vsE1             | 101    | Disabled | Disabled |
| vsE2             | 102    | Enabled  | Enabled  |
+------------------+--------+----------+----------+
```

Procedure 10-30
Enabling and disabling dot1x

You can:

- enable dot1x
- disable dot1x

Step **Action**

Enable dot1x

1 Enable dot1x:

```
dot1x auth enable
```

Disable dot1x

2 Disable dot1x:

```
dot1x auth disable
```

—end—

Procedure 10-31
Enabling and disabling dot1x authentication

You can:

- enable dot1x authentication
- disable dot1x authentication

Step **Action**

Enable dot1x authentication

1 Enable dot1x authentication:

```
dot1x auth enable port <port>
```

where

port <port>	is the port(s) to enable.

Disable dot1x authentication

2 Disable dot1x authentication:

```
dot1x auth disable port <port>
```

where

port <port>	is the port(s) to disable.

—end—

Procedure 10-32
Configuring dot1x authentication port attributes

Configure dot1x authentication port attributes.

Step Action

1 Configure dot1x authentication port attributes.

```
dot1x auth set port <port> {eapol-version <NUMBER: 1-2>}
{max-reauth-req <NUMBER: 1-10>} {reauthentication <on |
off>} {mode <auto | force-auth | force-unauth>} {quiet-
period <SECONDS: 1-65535>} {reauth-period <SECONDS: 1-
65535>} {server-timeout <SECONDS: 1-180>}
```

where

port <port>	is the port(s) to re-authenticate.
eapol-version <NUMBER: 1-2>	sets the EAPOL version. The default is 2.
max-reauth-req <NUMBER: 1-10>	sets the maximum authentication request. The default is 2.
mode <auto } force-auth | force-unauth>	sets the port control to either auto, forceauth or forceunauth. The default is auto.
reauthentication <on | off>	enables re-authentication. The default is on.
quiet-period <SECONDS: 1-65535>	sets the quiet period. The default is 60 seconds.
reauth-period <SECONDS: 1-65535>	sets the reauthentication period. The default is 3600.
server-timeout <SECONDS: 1-180>	sets the server timeout. The default is 30 seconds.

—end—

Example

This example configures dot1x authentication port attributes.

```
dot1x auth set port 5 eapol-version 3 max-reauth-req 10 mode force-auth
reauthentication on quiet-period 600 reauth-period 4000 server-timeout 150
```

Procedure 10-33
Displaying dot1x authentication information

You can display the:

- authenticator port configuration
- authenticator information per port

Step Action

Display authenticator port configuration

1 Display the authenticator port configuration:

```
dot1x auth show {statistics}
```

where

statistics	shows the authenticator statistics.

Disable authenticator information per port

2 Display the authenticator information per port:

```
dot1x auth show port <port>
```

where

port <port>	is the port(s) to show.

—end—

Example

These examples show output for the dot1x auth show command for port 2.

```
> dot1x auth show port 2

+--------------- DOT1X AUTHENTICATOR PORT 2 SUMMARY --------------+
| Parameter                    | Value                             |
+------------------------------+-----------------------------------+
| Admin State                  | Enabled                           |
| Operational State            | Enabled                           |
| PAE State                    | Authenticated                     |
| Controlled Port Status       | Authorized                        |
+------------------------------+-----------------------------------+
| Auth Mode                    | Auto                              |
| EAP Version                  | 2                                 |
| Quiet Period (seconds)       | 60                                |
| Server Timeout (seconds)     | 30                                |
| Reauthentication             | On                                |
| Reauth Period (seconds)      | 3600                              |
| Max Reauth Requests          | 2                                 |
+------------------------------+-----------------------------------+
+---------------------- DOT1X AUTHENTICATOR PORT 2 STATISTICS -----------------------+
| Port | Eapol      | Eapol      | Id Req     | Id Resp    | Request    | Response   |
|      | Frames Tx  | Frames Rx  | Frames Tx  | Frames Rx  | Frames Tx  | Frames Rx  |
+------+------------+------------+------------+------------+------------+------------+
|    2 |          6 |          5 |          3 |          2 |          3 |          4 |
+------+------------+------------+------------+------------+------------+------------+

+--------------- DOT1X AUTHENTICATOR PORT 2 SESSION STATISTICS ----------------+
| Parameter               | Value                                              |
+-------------------------+----------------------------------------------------+
| Frames Tx               | 136                                                |
| Frames Rx               | 136                                                |
| Octets Tx               | 30854                                              |
| Octets Rx               | 30854                                              |
| Sess Id                 | 386D67BD-00000001                                  |
| Session Time (seconds)  | 996                                                |
| Session Auth Method     | Remote Authentication Server                       |
| Session Terminate Cause | Not Terminated Yet                                 |
| Session Username        | ciena                                              |
+-------------------------+----------------------------------------------------+

+---------------------- DOT1X AUTHENTICATOR PORT 2 RADIUS STATISTICS ----------------------+
| Parameter             | Value                                                            |
+-----------------------+------------------------------------------------------------------+
| Requests              | 4                                                                |
| Access Accepts        | 1                                                                |
| Access Challenges     | 2                                                                |
| Access Rejects        | 0                                                                |
| Retransmissions       | 9                                                                |
| Bad Authenticators    | 0                                                                |
| Timeouts              | 9                                                                |
| Unknown Types         | 0                                                                |
| Packets Dropped       | 0                                                                |
+-----------------------+------------------------------------------------------------------+
| Last Server:          |                                                                  |
|    IP Address         | radserver                                                        |
|    Hostname           | 10.10.10.10                                                      |
|    Last Event         | Access Accept                                                    |
+-----------------------+------------------------------------------------------------------+
```

Procedure 10-34
Clearing authenticator statistics

You can clear:

- port authenticator statistics
- authenticator statistics

Step Action

To clear port authenticator statistics for a specified port

1 Clear port authenticator statistics:

```
dot1x auth clear port <port> {statistics}
```

where

port <port>	is the port(s) to clear.
statistics	is the statistics table

To clear authenticator statistics

2 Clear authenticator statistics:

```
dot1x auth clear {statistics}
```

where

statistics	is the statistics table

—end—

Procedure 10-35
Reauthenticating the port

Re-authenticating the port causes the authenticator to force the re-authentication of the supplicant.

Step **Action**

1 Force the re-authentication of the supplicant:

```
dot1x auth pae-port-reauth port <port>
```

where

port <port>	is the port(s) to re-authenticate.

—end—

Procedure 10-36
Resetting dot1x authentication port attributes

Reset dot1x authentication port attributes to default values.

Step **Action**

1 Reset dot1x authentication port attributes to default values:

```
dot1x auth unset port <port> [eapol-version] [max-reauth-
req] [mode] [reauthentication] [quiet-period] [reauth-
period]
```

where

port <port>	is the list of ports.
eapol-version	unsets the EAPOL version. The default is 2.
max-reauth-req	unsets the maximum authentication request. The default is 2.
mode	unsets the port control. The default is auto.
reauthentication	unsets re-authentication. The default is on.
quiet-period	unsets the quiet period. The default is 60 seconds.
reauth-period	unsets the reauthentication period. The default is 3600.
server-timeout	unsets the server timeout. The default is 30 seconds.

—end—

Example

This example resets dot1x authentication port attributes to their default values.

```
dot1x auth unset port 5 eapol-version max-reauth-req mode reauthentication
quiet-period reauth-period server-timeout
```

Procedure 10-37
Configuring the 802.1x supplicant for EAP-MD5

Configure the 802.1x supplicant for EAP-MD5.

CAUTION
Access to supplicant port
Enabling 802.1x operation blocks further access to the supplicant port until it has been authenticated. Make sure to configure all supplicant-specific settings *before* enabling 802.1x operation on the device, otherwise, the remaining configuration must be performed using a console port connection or through another port on the device that is also part of the device's management VLAN but is not configured as a supplicant.

Step **Action**

1 Establish a connection with the supplicant device.

2 Enable 802.1x operation:

```
dot1x enable
```

3 Configure the supplicant port:

```
dot1x supp set port <port> [authentication-period
<NUMBER: 1-65535>][cert-name <certificate-name>] [check-
cert-time <on | off>][eapol-version <NUMBER: 1-2>][eap-
method <eap-md5 | eap-tls>] [held-period <NUMBER: 1-
65535>] [echoless-password] [max-start <NUMBER: 1-65535>]
[minimum-tls-version <version>] [mutual-authentication
<on | off>] [ocsp <on | off>] [start-period <NUMBER: 1-
65535>] [username <String[15]>]
```

where

port <port> is the list of ports.

authentication-period <NUMBER: 1-65535> is the authentication period.

cert-name <certificate name> sets the name of the device certificate to use for EAP-TLS.

check-cert-time <on | off> determines if certificate dates are checked or ignored when and if the supplicate authenticates the server. Default is on.

eapol-version <NUMBER: 1-2> is the EAPOL version.

where

eap-method <eap-md5 | eap-tls>	selects the EAP-method. For this procedure, select EAP-MD5.
held-period <NUMBER: 1-65535>	is the held period.
echoless password	engages an echoless password collector
max-start <NUMBER: 1-65535>	is the maximum number of retries.
minimum-tls-version <version>	sets the minimum TLS version used for EAP-TLS. Options are • TLSv1.0 • TLSv1.1 • TLSv1.2
mutual-authentication <on|off>	determines if the supplicant authenticates the server. Default is off.
ocscp <on | off>	enables or disables OCSP stapling to validate peer certificates for EAP-TLS.
start-period <NUMBER: 1-65535>	is the start period.
[username <String[15]>]	is the username as it is configured on the remote authentication server. Text strings are case-sensitive.

4 Enable supplicant operation:

```
dot1x supp enable port <port>
```

where

port <port>	is the list of ports to enable.

The supplicant sends EAPOL start messages and looks for an authenticator.

—end—

Example

This example configures an 802.1x supplicant using EAP-MD5.

```
dot1x enable
dot1x supp set port 5 eap-method eap-md5
dot1x supp set port 5 echoless-password
Enter Password:
```

```
Verify Password:
dot1x supp set port 5 username myusername
dot1x supp enable port 5
```

Procedure 10-38
Configuring the 802.1x supplicant for EAP-TLS

Configure the 802.1x supplicant for EAP-TLS.

Note 1: EAP-TLS operation requires the installation of a device certificate and a private key signed by the CA certificate on your server. See the procedure, "Configuring and displaying supplicant device certificates on a port" on page 10-90.

Note 2: If mutual authentication is used, you must have already installed CA certificates. See the procedure, "Installing a trusted CA certificate" on page 10-84.

CAUTION

Blocked access to supplicant port

Enabling 802.1x operation blocks further access to the supplicant port until it has been authenticated. Make sure to configure all supplicant-specific settings *before* enabling 802.1x operation on the device, otherwise, the remaining configuration must be performed using a console port connection or through another port on the device that is also part of the device's management VLAN but is not configured as a supplicant.

Step **Action**

1 Establish a connection with the supplicant device.

2 Enable 802.1x operation:

```
dot1x enable
```

3 Configure the supplicant port:

```
dot1x supp set port <port> [authentication-period
<NUMBER: 1-65535>][cert-name <certificate-name>] [check-
cert-time <on | off>][eapol-version <NUMBER: 1-2>][eap-
method <eap-md5 | eap-tls>] [held-period <NUMBER: 1-
65535>] [echoless-password] [max-start <NUMBER: 1-65535>]
[minimum-tls-version <version> [mutual-authentication
<on | off>] [ocsp <on | off>] [start-period <NUMBER: 1-
65535>] [username <String[15]>]
```

where

port <port>
is the list of ports.

authentication-period <NUMBER: 1-65535>
is the authentication period.

cert-name <certificate name>
sets the name of the device certificate to use for EAP-TLS.

check-cert-time <on | off>
determines if certificate dates are checked or ignored when and if the supplicate authenticates the server. Default is on.

eapol-version <NUMBER: 1-2>
is the EAPOL version.

eap-method <eap-md5 | eap-tls>
selects the eap-method as EAP-MD5 or EAP-TLS. For this procedure, select EAP-TLS. Using EAP-TLS requires a supplicant device certificate. This certificate must already be installed. See “Creating and installing device certificates” on page 9-23.

held-period <NUMBER: 1-65535>
is the held period.

echoless password
engages an echoless password collector

max-start <NUMBER: 1-65535>
is the maximum number of retries.

minimum-tls-version <version>
sets the minimum TLS version used for EAP-TLS. Options are

- TLSv1.0
- TLSv1.1
- TLSv1.2

mutual-authentication <on|off>
causes the supplicant to authenticate or to not authenticate the server during EAP-TLS. Turning mutual authentication on requires CA certificates. These certificates must already be installed. See “Installing a trusted CA certificate” on page 10-84.

where

ocscp <on | off> enables or disables OCSP stapling to validate peer certificates for EAP-TLS.

start-period <NUMBER: 1-65535> is the start period.

[username <String[15]>] is the username as it is configured on the remote authentication server. Text strings are case-sensitive.

4 Enable supplicant operation:

```
dot1x supp enable port <port>
```

where

port <port> is the list of ports to enable.

The supplicant sends EAPOL start messages and looks for an authenticator.

—end—

Example

This example configures an 802.1x supplicant using EAP-TLS.

```
dot1x enable
dot1x supp set port 4 eap-method eap-tls
dot1x supp set port 4 username portIdentity
dot1x supp set port 4 mutual-auth on
dot1x supp set port 4 cert-name myCertName
dot1x supp set port 4 check-cert-time-on
dot1x supp enable
```

Procedure 10-39
Displaying dot1x global information

You can display dot1x global information:

Step	Action
1	Display dot1x global information: `dot1x show`

—end—

Example

This example shows output from the dot1x show command.

```
> dot1x show

+---- DOT1X GLOBAL STATUS----+
| Parameter     | Value       |
+---------------+------------+
| Admin State   | Enabled    |
+---------------+------------+

+----------------------------- DOT1X PORT STATE ------------------------------+
| Port | Port Role     | Admin    | Oper     | PAE            | Controlled    |
|      | (Auth/Supp)   | State    | State    | State          | Port Status   |
+------+---------------+----------+----------+----------------+---------------+
|    1 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    2 | Authenticator | Enabled  | Enabled  | Authenticated  | Authorized    |
|    3 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    4 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    5 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    6 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    7 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    8 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|    9 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|   10 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|   11 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
|   12 | None          | Disabled | Disabled | Disconnected   | Unauthorized  |
+------+---------------+----------+----------+----------------+---------------+
```

Procedure 10-40
Displaying CA certificates

Shows all installed CA certificates or a specific CA certificate identified by its hash value.

Step **Action**

1 Display CA certificates:

```
system security ca-certificate show [ca-cert-hash <ca-cert-hash>]
```

where

ca-cert-hash <ca-cert-hash> is an optional argument that allows a specific certificate to be shown based on its hash value

—end—

Example

This example shows output from the system security pkix ca show command.

```
> system security pkix ca show

+------------------------------ CA CERTIFICATES ----------------------------+
| Parameter           | Value                                               |
+---------------------+-----------------------------------------------------+
| Certificate Hash    | 4819cdba                                            |
| Subject Common Name | haxv-lab02-06.ciena.com                             |
| Issuer Common Name  | haxv-lab02-06.ciena.com                             |
| Valid To            | Aug 17 16:19:35 2018 GMT (11 months)                |
+---------------------+-----------------------------------------------------+
```

Procedure 10-41
Installing a trusted CA certificate

Install a trusted CA certificate from an external FTP server. CA Certificates are used to validate peer certificates.

Step **Action**

1 Install the CA certificate (where is the FTP server IP address, is the certificate name and alice is the login-id):

```
system security pkix ca install ftp-server <IP address or
host name> filename <String[1..127]> login-id
<String[1..32]> echoless-password
```

2 Verify the installation of the certificate:

```
system security pkix ca show
```

—end—

Example

This example shows the installation of a CA certificate “ca.cert.pem” from an FTP server with an IP address of 10.10.10.10, for a user named alice. The password is not shown since echoless password was chosen:

```
> system security pkix ca install ftp-server 10.10.10.10 filename ca.cert.pem
login-id alice echoless-password
 Enter Password:

> system security pkix ca show

+--------------------------- CA CERTIFICATES ----------------------------+
| Parameter            | Value                                            |
+---------------------+--------------------------------------------------+
| Certificate Hash     | 5a9530f5                                         |
| Subject Common Name  | MyServerCA                                       |
| Issuer Common Name   | MyServerCA                                       |
| Valid To             | Jul 29 15:46:41 2017 GMT                         |
+---------------------+--------------------------------------------------+
```

This example installs a CA certificate from an SFTP server. A login ID is specified. The CLI prompts the user for the server password without echoing the password characters to the screen.

```
> system security pkix ca install sftp-server MyServer filename dot1xCA.pem
login-id testUser echoless password
Enter Password:[password is entered but not echoed]
Verify Password:[password is entered but not echoed]
```

This example installs a CA certificate from an HTTP server.

```
> system security pkix ca install url http://MyServer/dot1xCA.pem
```

Procedure 10-42
Uninstalling CA certificates

This procedure uninstalls CA certificates.

You must have super user privileges to perform this procedure.

Step **Action**

1 Uninstall CA certificates:

```
system security pkix ca uninstall ca-cert-hash <CA
certificate hash[1..8]>
```

where

ca-cert-hash <CA certificate hash[1..8]>	is the hash value of the CA certificate that you wish to uninstall.

—end—

Example

This example uninstalls a CA certificate.

```
> system security pkix ca uninstall ca-cert-hash 9741086f
```

Procedure 10-43
Installing certificate revocation lists

This procedure installs certificate revocation lists (CRLs).

You must have super user privileges to perform this procedure.

Step **Action**

1 Install CRLs:

```
system security pkix crl install {filename <String>}
{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>]}
[force] {url <STRING>|{{filename <STRING[1..127]>}
```

where

filename <string>	is the authentication key filename.
default-server	use the default xFTP server.
default-ftp-server	use the default FTP server.
default-tftp-server	use the default TFTP server.
default sftp-server	use 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 sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.

where

echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.
force	is an optional keyword that is used to overwrite any existing certificate. If force is not used, the existing certificate is not overwritten. If you use force, specify the keywords for the server, such as tftp-server or sftp-server.
url <STRING>	is the remote file URL. A login ID may be specified to access the URL host (HTTP server).

—end—

Example

This example installs a CRL from an HTTP server.

```
> system security pkix crl install url http://MyServer/dot1xCRL.pem
```

Procedure 10-44
Uninstalling certificate revocation lists

This procedure uninstalls CRLs.

You must have super user privileges to perform this procedure.

Step	Action
1	Uninstall a CRL:

```
system security pkix crl uninstall crl-hash <CRL
hash[1..8]>
```

where

crl-hash <CRL hash[1..8]>	is the hash value of the CRL that you wish to uninstall.

—end—

Procedure 10-45
Displaying certificate revocation lists

Shows all installed CRLs or a specific CRL identified by its hash value.

Step **Action**

1 Display CRLs:

```
system security pkix crl show [crl-hash<CRL hash[1..8]>]
```

where

crl-hash<CRL hash[1..8]> is an optional argument that allows a specific CRL to be shown based on its hash value

—end—

Example

This example shows the output from the system security pkix crl show command.

```
> system security pkix crl show
+----------------------- CERTIFICATE REVOCATION LISTS -----------------------+
| Parameter             | Value                                              |
+-----------------------+----------------------------------------------------+
| No CRLs               |                                                    |
+-----------------------+----------------------------------------------------+
```

Procedure 10-46
Configuring and displaying supplicant device certificates on a port

Configure and display supplicant device certificates on a port.

> ***Note:*** You must have super user privileges to perform this procedure.

Step	Action
1	Install a device certificate (see "Creating and installing device certificates" on page 9-23).
2	Configure dot1x to use the created certificate using the cert-name used when creating/installing the device certificate: `dot1x supp set port <port-object-list> cert-name <cert-name>`
3	Verify the device certificate on a port `dot1x supp show port <port-object-list> certificate`

Example

This example shows the details of the dot1x supplicant certificate installed on port 1 in slot 1:

```
> dot1x supp set port 1/1 cert-name test
> dot1x supp show port 1/1 certificate

+-------------- DOT1X PORT 1/1 DEVICE CERTIFICATE ---------------+
| Parameter            | Value                                   |
+----------------------+-----------------------------------------+
| Certificate Name     | test                                    |
+----------------------+-----------------------------------------+
| Private Key          | Present                                 |
| Key Type             | RSA (2048)                              |
+----------------------+-----------------------------------------+
| Device Certificate   |                                         |
|  Subject Common Name | SaosCertificate                         |
|  Issuer Common Name  | MyCA                                    |
|  Valid To            | Oct  5 15:02:01 2018 GMT (11 months)    |
+----------------------+-----------------------------------------+
```

Procedure 10-47
Displaying supplicant information for a port

Display supplicant information per port to verify the configuration. You must have super user privileges to perform this procedure.

Step	Action
1	Display supplicant information per port: `dot1x supp show port {<port-object-list>}`

where

port <port-object-list>	is the port with the device certificates that you wish to view.

—end—

Example

This example shows output for the dot1x sup show command for port 3:

```
>dot1x supp show port 3

+--------------- DOT1X SUPPLICANT PORT 3 SUMMARY ----------------+
| Parameter                   | Value                            |
+-----------------------------+----------------------------------+
| Admin State                 | Disabled                         |
| Operational State           | Disabled                         |
| PAE State                   | Disconnected                     |
| Controlled Port Status      | Unauthorized                     |
+-----------------------------+----------------------------------+
| Start Period (sec)          | 30                               |
| Held Period (sec)           | 60                               |
| Auth Period (sec)           | 30                               |
| Max Start                   | 2                                |
+-----------------------------+----------------------------------+
| Username                    |                                  |
| EAP Version                 | 2                                |
| EAP Method                  | EAP-MD5                          |
| MD5 Password                | Unset                            |
| Port Device Certificate/Key | Not Present                      |
| Mutual Auth Admin State     | Disabled                         |
| Mutual Auth Oper State      | Disabled                         |
| Check Cert Time Admin State | Enabled                          |
| Check Cert Time Oper State  | Disabled                         |
+-----------------------------+----------------------------------+

+------------------------ DOT1X SUPPLICANT PORT 3 STATISTICS ------------------------+
| Port |    Eapol    |    Eapol    |   Id Req    |   Id Resp   |   Request   |  Response   |
|      |  Frames Tx  |  Frames Rx  |  Frames Rx  |  Frames Tx  |  Frames Rx  |  Frames Tx  |
+------+-------------+-------------+-------------+-------------+-------------+-------------+
|    3 |           0 |           0 |           0 |           0 |           0 |           0 |
+------+-------------+-------------+-------------+-------------+-------------+-------------+
```

Procedure 10-48
Restarting the authenticator or supplicant on a port

Restart the authenticator or supplicant on a given port.

Step	Action
1	Restart the authenticator or supplicant on a given port.

```
dot1x pae-port-initialize port <port>
```

where

port <port>	is the port(s) to initialize.

—end—

Procedure 10-49
Configuring a PC as a supplicant

Configure a personal computer (PC) with an 802.1x-capable network interface card (NIC) when you want to use the PC as s a supplicant. Using a device configured as an authenticator, the PC can be authenticated to access the network.

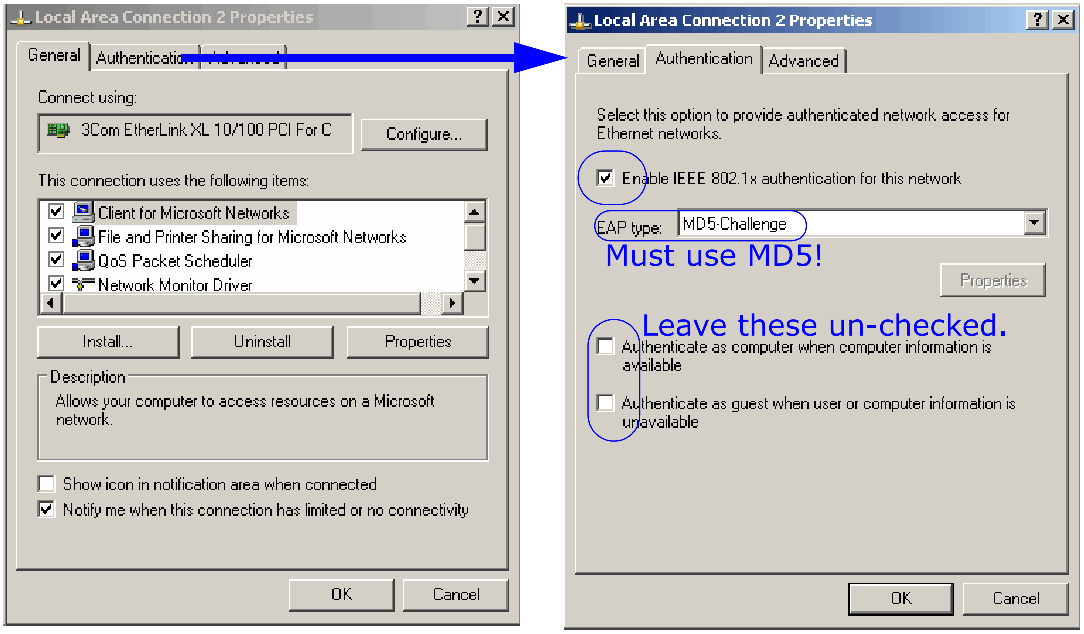
The operating system of both the NIC and the PC must support 802.1x operation. Some NICs provide 802.1x operation while others do not. If an “Authentication” tab is not displayed in the NIC’s configuration settings, 802.1x is probably not supported. Refer to the vendor documentation for the NIC to determine capabilities and operating system requirements. Refer to http://windows.microsoft.com/en-us/windows-vista/enable-802-1x-authentication for PC operating system information.

Prerequisites

- NIC is enabled
- one of the following has been performed:
  - — NIC is configured with a static IP address that is in the subnet of the network
  - — NIC is configured to use DHCP to obtain an IP address and a DHCP server is reachable on the network

Step	Action
1	Open the properties window for the NIC by right-clicking on the entry for the NIC being used, and selecting Properties.
2	Click the Authentication tab.

Figure 10-3
Local Area Connection Properties



Connect using:

3Com EtherLink XL 10/100 PCI For C

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Network Monitor Driver

Description
Allows your computer to access resources on a Microsoft network.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: MD5-Challenge

Must use MD5!

Leave these un-checked.

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

3 Check the box next to “Enable IEEE 802.1x authentication for this network.”

4 Select MD5-Challenge for the EAP Type.

5 Uncheck any other boxes that may be checked.

6 Click OK.

7 Close the NIC properties window.

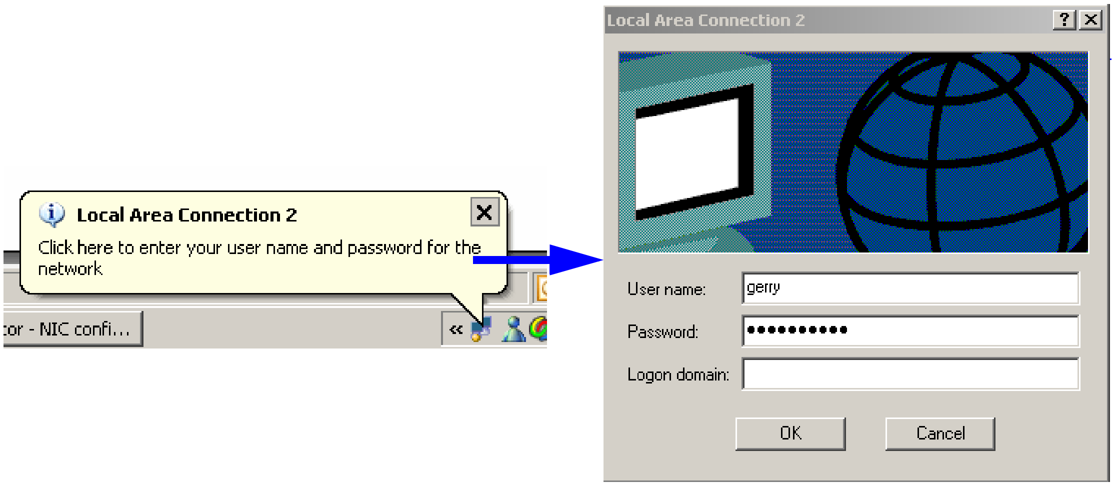
8 Connect the PC to the port configured as the authenticator on the device connected to the network.

After several seconds, the PC displays an alert regarding entering user credentials.

9 Click on the alert to display the entry window.

10 Enter the user name and password exactly as it is entered on the authentication server and click OK.

Figure 10-4
Authenticating the PC



Local Area Connection 2

Click here to enter your user name and password for the network

User name: gerry

Password: ••••••••••

Logon domain:

—end—

Procedure 10-50
Troubleshooting 802.1x

Troubleshoot 802.1x if a supplicant fails to authenticate when put into service or when the supplicant cannot be contacted after it successfully authenticates.

Step	Action
1	Check that the physical ports on the devices that are configured as the supplicant and the authenticator have a direct physical connection to each other. The only exception to this is if control frame tunneling is configured to tunnel 802.1x EAPOL frames through any intermediate device(s) connecting the supplicant to the authenticator.
2	If the supplicant is configured to obtain its IP address from a DHCP server, that server must be accessible once the supplicant has been authenticated.
3	Make sure that global 802.1x operation is enabled on the supplicant and on the authenticator.
4	Verify that MD5 encryption is being used by the authentication server. Other types of encryption, such as Protected EAP (PEAP), are not supported.
5	Make sure that the supplicant, authenticator, and authentication server are on the same VLAN to communicate (unless a router exists between the switch and the server. ***Note:*** The EAPOL messages sent by the supplicant are not 802.1q tagged, therefore the supplicant can successfully authenticate without being on the same VLAN as the authenticator or the authentication server. Once authentication is successful, the supplicant cannot communicate with the authenticator if it is on a different VLAN.
6	Use the `ping` command to verify that the authenticator can communicate with the authentication server.
7	Verify that the authentication server's authentication port number is the same number specified in the supplicant's settings.
8	Verify that the RADIUS key specified matches the key configured on the authentication server.
9	Verify that the user name and password specified for the supplicant are *exactly* the same as they are entered in the authentication server's user list (including the use of lower and upper case characters.

—end—

Procedure 10-51
Configuring SNMP community mapping

Configure SNMP community mapping so that an SNMP engine can send and receive SNMPv1 and SNMPv2c messages. Create at least one SNMPv3 community.

> ***Note:*** To configure SNMPv3 encryption and authentication, the Advanced Security feature license must be installed.

Step **Action**

1 Create an entry in the *snmpCommunityTable*:

```
snmp create community-index <String[32]> {community
<String[64]>} {sec-name <String[32]>} [transport-tag
<String[32]>]
```

where

community-index <String[32]>	is a text string of up to 32 characters that is unique among SNMP community-map entries.
community <String[64]>	is a community string of up to 64 characters, which can be a readable string or a hexadecimal representation containing unprintable characters.
sec-name <String[32]>	is a text string of up to 32 characters which identifies the security name for the community. This string must appear in at least one security-to-group table entry to assign the community to an access control group.
transport-tag <String[32]>	is a text string of up to 32 characters to select a set of entries in the SNMP target table for source address checking. Entries in the SNMP target table are selected if the value of transport-tag appears in list of tags in the target table

2 Verify that the new entry was created:

```
snmp show community-map
```

3 Create an entry in the *vacmAccessTable*:

```
snmp create access-entry <String[32]> {sec-model
<v1|v2c|v3>}{sec-level
<noAuth|authNoPriv|authWithPriv>}[read-view
<String[64]>][write-view <String[64]>][notify-view
<String[64]>]
```

where

access-entry <String[32]>	is the name of the access policy
sec-model <v1|v2c|v3>	is the security model for access entry.
sec-level <noAuth| authNoPriv| authWithPriv>	is the security level.
read-view <String[64]>	is the read view name. Left unspecified, the default value is '1.3.6.1' which is every object under internet sub tree.
write-view <String[64]	is the write view name. The default value is 'null OID', where nothing is included for write access.
notify-view <String[64]>	is the notify view name. The default value is 'null OID', nothing is included for notify access.

4 Verify that the new entry was created:

```
snmp show access-entry
```

5 Create an entry in the *vacmSecurityToGroupTable*:

```
snmp security-to-group attach user <String[32]> sec-model
<v1|v2c|v3> group <String[32]>
```

where

user <String[32]>	is the name of the user.
sec-model <v1|v2c|v3>	is the security model for access entry.
group <String[32]>	is the name of the group.

6 Verify that the new entry was created.

```
snmp show security-to-group
```

7 Create an entry in the *vacmViewTreeFamilyTable*:

```
snmp create viewtree <String[32]> {sub-tree <String[64]>}
{type <include|exclude>}
```

where

viewtree <String[32]> is the name of the viewtree.

sub-tree <String[64]> is the object identifier (OID) of the MIB.

type <include|exclude> sets whether the specified sub-tree is to be included or excluded from the view.

8 Verify that the new entry was created:

```
snmp show viewtree
```

—end—

Example

Create an entry in the *snmpCommunityTable*.

```
snmp create community-index comm1 community mycommunity
sec-name user1
```

Verify that the new entry was created.

```
snmp show community-map

+----------------+----------------+----------------+----------------+
| CommunityIndex | CommunityName  | SecName        | TransportTag   |
+----------------+----------------+---------------- ----------------+
| comm1          | mycommunity    | user1          |                |
| t0000000       | public         | public         | anywhereTag    |
| t0000001       | private        | private        | anywhereTag    |
+----------------+----------------+----------------|----------------+
```

Create an entry in the *vacmAccessTable*.

```
snmp create access-entry group1 sec-model v1 sec-level
noAuth read-view viewtree1
```

Verify that the new entry was created.

```
snmp show access-entry

+------------+----------+----------+----------+-----------+-----------+
| GroupName  | SecModel | SecLevel | ReadView | WriteView | NotifView |
+------------+----------+----------+----------+-----------+-----------+
| group1     | v1       | noAu     | viewtree1|           |           |
| public     | v1       | noAu     | V12cView |           | V12cView  |
| public     | v2c      | noAu     | V12cView |           | V12cView  |
| private    | v1       | noAu     | V12cView | V12cView  | V12cView  |
| private    | v2c      | noAu     | V12cView | V12cView  | V12cView  |
+------------+----------+----------+----------+-----------+-----------+
```

Create an entry in the *vacmSecurityToGroupTable*.

```
snmp security-to-group attach user user1 sec-model v1
group group1
```

Verify that the new entry was created.

```
snmp show security-to-group

+------------------------+----------+-------------------+
| UserName               | SecModel | GroupName         |
+------------------------+----------+-------------------+
| user1                  | v1       | group1            |
| public                 | v1       | public            |
| private                | v1       | private           |
| public                 | v2c      | public            |
| private                | v2c      | private           |
+------------------------+----------+-------------------+
```

Create an entry in the *vacmViewTreeFamilyTable*.

```
snmp create viewtree viewtree1 sub-tree mgmt type include
```

Verify that the new entry was created.

```
snmp show viewtree

+----------------------------+------------------------+----------+
| ViewTreeName               | SubTree                | Type     |
+----------------------------+------------------------+----------+
| V12cView                   | iso                    | include  |
| V12cView                   | snmpResearch           | exclude  |
| viewtree1                  | mgmt                   | include  |
+----------------------------+------------------------+----------+
```

Procedure 10-52
Creating and attaching an SNMPv3 user to an SNMPv3 access entry group

Create and attach an SNMPv3 user to an SNMPv3 access entry group to provide the View-based Access Control Model.

Step	Action

1 Create an SNMPv3 user with an authentication protocol, privacy protocol, authentication password, and privacy password.

```
snmp create user <user> {auth-protocol <noauth|md5|sha>}
[echoless-auth-password] [priv-protocol <aes-
128|des|3des|noPriv>] [echoless-priv-password] [auth-
secret <String[40]>] [priv-secret <String[64]>] [engine-
id <SNMP EngineID:XX:XX..(5-32 octets)
Default:LocalSnmpEngineId>]
```

where

user <user>	is the SNMP user name.
auth-protocol <noauth | md5 | sha>	is the Authentication Protocol.
echoless-auth-password	collects authentication password interactively.
priv-protocol <aes-128|des|3des|noPriv>	is the Privacy Protocol.
echoless-priv-password	collects privacy password interactively.
auth-secret <String[40]>	sets the password using a pre-encrypted string.
priv-secret <String[64]>	sets the SNMP user priv password using a pre-encrypted string.
engine-id<SNMP EngineID:XX:XX..(5-32 octets) Default: LocalSnmp EngineId>	is the SNMP engine ID.

2 Verify that the new entry was created.

```
snmp show user
```

3 Create a view tree entry in the *vacmViewTreeFamilyTable* with a sub-tree that can be viewed:

```
snmp create viewtree <viewtree> {sub-tree <String[64]>}
{type <include|exclude>}
```

where

viewtree <viewtree>	is the SNMP view tree name.
sub-tree <String[64]>	is the sub-tree MIB OID.
type <include | exclude>	indicates whether to include or exclude the tree type.

4 Verify that the new entry was created:

```
snmp show viewtree
```

5 Create an access policy in the *vacmAccessTable* with a v3 security model.

```
snmp create access-entry <access-entry> {sec-model
<v1|v2c|v3>}{sec-level <noAuth|authNoPriv|authWithPriv>}
[read-view <String[64]>][write-view
<String[64]>][notify-view <String[64]>]
```

where

access-entry <access-entry>	is the SNMP access entry.
sec-model <v1 | v2c | v3>	is the security model for access entry.
sec-level <noAuth | authNoPriv | authWithPriv>	is the security level.
read-view <String[64]>	is the read view name.
write-view <String[64]>	is the write view name.
notify-view <String[64]>	is the notify view name

6 Verify that the new entry was created:

```
snmp show access-entry
```

7 Attach the SNMPv3 user to an SNMPv3 access group using the *vacmSecurityToGroupTable*:

```
snmp security-to-group attach user <user> {sec-model
<v1|v2c|v3>} {group <String[32]>}
```

where

user <user> is the SNMP user name.

sec-model <v1|v2c|v3> is the security model for the user.

group <String[32]> is the SNMP group name.

8 Verify that the new entry was created:

```
snmp show security-to-group
```

—end—

Example

Create an SNMPv3 user with an authentication protocol, echoless password, privacy protocol, authentication password, and privacy password.

```
> snmp create user SNMPv3_User auth-protocol md5 echoless-auth-password priv-
protocol des echoless-priv-password auth-password SNMPv3_password1 priv-
password SNMPv3_password2
```

Verify that the new entry was created.

```
> snmp show user

+--------------+-----------+----------+------------------------------------+
| UserName     | AuthProt  | PrivProt |Engine ID                           |
+--------------+-----------+-----------------------------------------------+
| public       | noAuth    | noPriv   |80:00:04:f7:05:00:03:18:55:71:d0:00 |
| private      | noAuth    | noPriv   |80:00:04:f7:05:00:03:18:55:71:d0:00 |
| SNMPv3_User  | md5       | des      |80:00:04:f7:05:00:03:18:55:71:d0:00 |
+--------------+-----------+-----------------------------------------------+
```

Create a view tree entry in the *vacmViewTreeFamilyTable* with a sub-tree that can be viewed.

```
> snmp create viewtree SNMPv3_view sub-tree mgmt type include
```

Verify that the new entry was created.

```
> snmp show viewtree

+----------------------------+------------------------+----------+
| ViewTreeName               | SubTree                | Type     |
+----------------------------+------------------------+----------+
| V12cView                   | iso                    | include  |
| V12cView                   | snmpResearch           | exclude  |
| SNMPv3_view                | mgmt                   | include  |
+----------------------------+------------------------+----------+
```

Create an access policy in the *vacmAccessTable* with a v3 security model. Include a security level with authorization and privileges. Also include a read view, write view, and notify view.

```
> snmp create access-entry SNMPv3_Group sec-model v3 sec-level authWithPriv
read-view SNMPv3_view write-view SNMPv3_view notify-view SNMPv3_view
```

Verify that the new entry was created.

```
> snmp show access-entry

+--------------+-----------+----------+-------------+-------------+-------------+
| GroupName    | SecModel  | SecLevel | ReadView    | WriteView   | NotifView   |
+--------------+-----------+----------+-------------+-------------+-------------+
| public       | v1        | noAuth   | V12cView    |             | V12cView    |
| public       | v2c       | noAuth   | V12cView    |             | V12cView    |
| private      | v1        | noAuth   | V12cView    | V12cView    | V12cView    |
| private      | v2c       | noAuth   | V12cView    | V12cView    | V12cView    |
| SNMPv3_Group | usm       | AuthWtPv | SNMPv3_view | SNMPv3_view | SNMPv3_view |
+--------------+-----------+----------+-------------+-------------+-------------+
```

Attach the SNMPv3 user to an SNMPv3 access group using the *vacmSecurityToGroupTable*.

```
> snmp security-to-group attach user SNMPv3_User sec-model v3 group
SNMPv3_Group
```

Verify that the new entry was created.

```
> snmp show security-to-group

+------------------------+----------+------------------+
| UserName               | SecModel | GroupName        |
+------------------------+----------+------------------+
| public                 | v1       | public           |
| private                | v1       | private          |
| public                 | v2c      | public           |
| private                | v2c      | private          |
| SNMPv3_User            | v3       | SNMPv3_Group     |
+------------------------+----------+------------------+
```

Enhanced security

Many of the SAOS switch security features are enabled by default. There are several features that can be configured to make the switches more secure and/or to make the switches more compliant with the standards established in Common Criteria security, Joint Interoperability Test Command (JITC), and the Security Technical Implementation Guides (STIGs)

SAOS devices support normal and enhanced security mode. Enhanced security mode supports the standards established in JITC and STIGs.

> **WARNING**
> **Enhanced Security Mode**
> Enhanced security mode is only required if you need to run a device in a JITC compliant environment. Do not put a device in enhanced security mode if this is not required. Operate devices in normal mode for non-JITC operations.

Kernel and SAOS

In enhanced security mode, the hardened kernel is enabled on the device, resulting in kernel-level changes. Hardened kernel disables access to most of the file systems and prevents users from editing or deleting files.The hardened kernel is not enabled in normal mode.

SAOS level changes involve the configuration of the device. In normal mode, public and private SNMP communities are created by default. In contrast, SNMP communities are not allowed in enhanced security mode.

User accounts

In normal mode, four default accounts are provided. in enhanced security mode, only the su account is created by default. Users typically change the password to this account and create new accounts at the desired privilege levels. For more information, see “Administration fundamentals” on page 2-1.

The user may also configure password complexity settings to require passwords to be of a minimum length and include special characters or upper case letters. These settings can be configured to the desired values on a device at any time after deployment. Requirements/rules can be set locally or using RADIUS TACACS servers.

UBOOT challenge response

The boot procedure for a SAOS device starts the UBOOT process when the system is powered up. UBOOT then launches the kernel, which launches the SAOS application. In normal mode, a user with physical access to the serial console can access UBOOT when the device is reset. UBOOT access in enhanced security mode is protected by a challenge-response generated by a program maintained by Ciena.

Login banner

In normal mode, the login banner is the default Ciena banner. By default, a warning banner is displayed in enhanced security mode that overrides the normal mode login banner file.

Enhanced security mode displays a DoD mandated banner that warns any unauthorized user not to proceed. It also warns authorized and unauthorized users that access to the device is subject to monitoring to detect any unauthorized usage. The required banner follows:

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See User
Agreement for details.
```

Auditing

In enhanced security mode, the hardened kernel logs events. The logs are used to audit security events and assist in security profile management. These logs can be used to

- change the user profile
- enable an account
- as a notification of a possible security violation

FIPS

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. and Canadian government certification that defines the requirements that cryptographic modules must follow. FIPS specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system.

FIPS compliant encryption is used in enhanced security mode. The FIPS code is built and used in the OpenSSL package. OpenSSL FIPS Object Module is designed for compatibility with OpenSSL, which is the library used for cryptography purposes. The same version of the OpenSSL package is used regardless of whether normal mode or enhanced security mode is used. For enhanced security mode, a self-test is enabled and run on all subsequent reboots. An error log is reported if the self-test fails.

FIPS-140-2 is automatically enabled in enhanced security mode for OpenSSH/SSL.

SSHv2 and SNMPv3 are only FIPS-140-2 compliant when the system’s encryption mode has been configured for compliance. SSHv2 and SNMPv3 are not FIPS compliant by default.

Any process that uses any of these algorithms for crytographic purposes is considered non-FIPS compliant:

- Rivest Cipher 4 (RC4)
- Message Digest (MD5)
- Keyed-Hash Message Authentication Code (HMAC) MD5
- Data Encryption Standard (DES)

In normal mode, the `system security set encryption-mode fips-140-2` command provides an option to enter FIPS mode, which automatically selects the cipher and MAC settings and limits these to FIPS approved. The user has the option to select FIPS mode while in normal mode. In enhanced mode, FIPS mode is automatically enabled.

FIPS procedures are:

- “Configuring the encryption mode” on page 11-21
- “Displaying the security configuration” on page 11-20

Firewall

In enhanced security mode, the firewall is enabled. All ports are closed with the exception of those needed for enabled services.

Network Time Protocol client authentication

In enhanced security mode, MD5 is disabled for Network Time Protocol (NTP) client authentication. SHA1 is used for NTP client authentication.

SNMP AES and 3DES encryption

Enhanced security mode supports AES-128 and 3DES encryption for SNMPv3 when creating users.

The procedure for SNMP AES and 3DES encryption is:

- “Creating and attaching an SNMPv3 user to an SNMPv3 access entry group” on page 10-101

Configuration differences

Some SAOS default configurations are different between normal mode and enhanced security mode. When set to enhanced security mode, the required default settings are automatically applied.

The default enhanced security mode changes include:

- turn off zero-touch provisioning
- disable default remote interface
- disable DHCP and DHCPv6
- remove all ports from VLAN1
- delete SNMP public and private communities
- apply enhanced security SSH settings
- disable Telnet server and client
- delete the default limited, admin, and diag accounts
- disable all ports by default
- remove the ability to configure non-FIPS encryption wherever it can be used (MD5, DES)

This table compares the configuration changes.

Table 11-1
Configuration changes

Feature	Normal mode	Enhanced security mode
Default user accounts	Limited, admin, su, and diag default accounts are created.	Only the default su account is available. Limited, admin, and diag user accounts are deleted.
DHCP and DHCPv6 client	Admin is enabled.	Admin is disabled.
FIPS-140-2 compliance	Disabled by default, but it is selectable.	Open SSL/SSH libraries are set to FIPS mode which allows only FIPS compliant ciphers and encryption. FIPS cannot be disabled.
Diag shell commands	Available	Limited to /bin/df, ls, cat, chmod cp, mkdir, mv, pwd, rm, rmdir, ping, ping6, ps, /usr/bin/scp, traceroute, traceroute6, telnet, tput, tftp, ssh, /ciena/bin/leos, /ciena/scripts/heapsize
directory access	All	Restricted to /dev, /dev, /dev/pts r, /dev/tty, rw, /proc/ /fd/ r, /proc/meminfo r, /mnt/sysfs, /mnt/sysfs/* rwcd
Enhanced security kernel	Hardened kernel is disabled.	Hardened kernel is enabled and limited access to directories, files and certain diagnostic commands.
FIPS-140-2 compliance	Disabled by default, but it is selectable.	Open SSL/SSH libraries are set to FIPS compliant ciphers and encryption, FIPs cannot be disabled.
ICMP accept redirects IPv4/IPv6	On	Off
ICMP echo ignore broadcast (IPv4/IPv6)	On	Off
ICMP port unreachable (IPv4/IPv6)	On	Off
Login banner	The login banner is the Ciena banner by default.	The login banner is replaced by the DoD-compliant JITC banner.
NTP authentication	MD5 and SHA-1 authentication are allowed.	NTP MD5 authentication is disabled. Only SHA-1 authentication can be used.
Port default Admin state	Admin is enabled.	Admin is disabled.

Table 11-1 Configuration changes

Feature	Normal mode	Enhanced security mode
Remote interface	Admin enabled	Admin disabled
SNMP Auth and Priv protocol settings	MD5, DES, AES and 3DES are available.	Non-FIPS-compliant methods (MD5, DES) are disabled. Users are limited to AES and 3DES.
SNMP default communities	Public and private default communities are created.	No default communities are created. Public and private default communities are deleted.
SSH client alive interval	0	60 seconds
SSH rekey timeout	0	3600 seconds
SSH rekey limit	0	1G
SSH client keep alive	On	Off
SSH client TCP forwarding	On	Off
SSH strict modes	Off	On
SSH maximum shared sessions	10	1
State dump	Available	Available
system shell set login-banner-file	Available	Not available.
system shell set welcome-banner-file	Available	Not available
TCPDUMP	Available	Not available
Telnet	Enabled	Disabled
UBOOT challenge response access	Disabled	Enabled.
User kill	Uses process identifier (PID)	Uses session identifier (SID)
User write CLI command	Available	Not available
VLAN1 ports	Ports are members of VLAN 1 and VLAN 127.	All ports are removed from VLAN 1.
zero touch provisioning	Enabled	Disabled

Enhanced security mode

> **WARNING**
> **Enhanced Security Mode**
> Enhanced security mode is only required if you need to run a device in a JITC compliant environment. Do not put a device in enhanced security mode if this is not required. Operate devices in normal mode for non-JITC operations.

Enhanced security mode is required for SAOS devices that must operate as a JITC compliant device. Devices that are not required to operate in enhanced or JITC mode operate in normal mode. The device security mode can be set to normal or enhanced by means of the CLI. When the device is installed, you must go into the device through the console port and use the CLI to change the security mode from normal to enhanced.

Setting the device to enhanced security mode requires a reset to factory defaults. A reset to factory defaults does not change the enhanced security mode setting.

The procedure for enhanced security mode is:

- “Setting the security mode” on page 11-22.

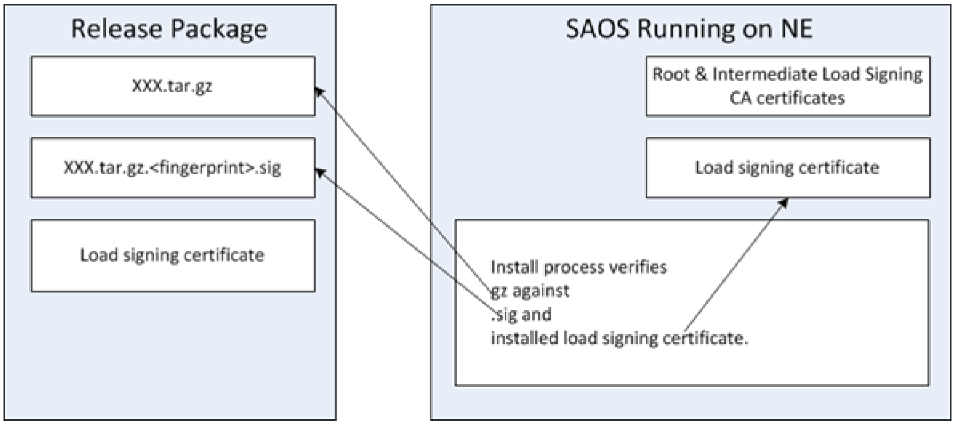
Software signing

Security standards such as Joint Interoperability Test Command (JITC) and Common Criteria required signed software packages to prevent the installation of unauthorized software.

A signed software load includes a signed hash of the rest of the software. The signature can be created with an X.509 certificate authority (CA) and a private key. Software signing can be verified against the public key in the certificate.

During the software installation process, the release and signature file is pre-checked against a copy of the CA certificate used to sign the software. SAOS looks for a .sig file that corresponds to a .gz file with a fingerprint matching the installed load signing certificate. Both files are used to verify the .gz file. If the release does not pass the check, it is not installed. This figure describes the software signature checking.

Figure 11-1
Software signing



Software signing can be enabled or disabled by users with super privileges. Software signing is disabled by default.

The procedure for software signing is:

- "Enabling and disabling software signature checking" on page 11-26.

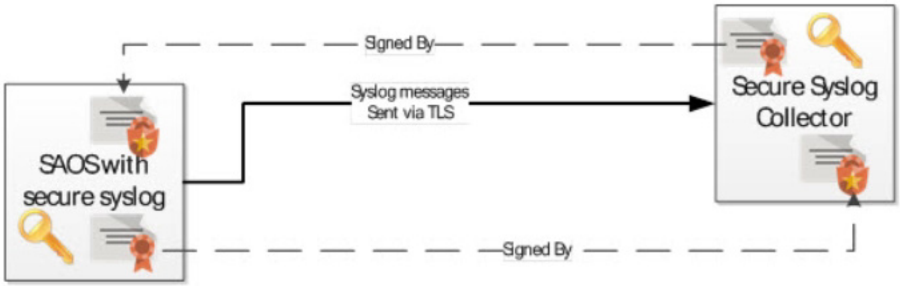
Secure Syslog (TLS Transport)

RFC 5425 specifies TLS transport mapping for Syslog. This allows originators and collectors to authenticate each other with signed X.509 digital certificates, providing authentication and secure transmission of Syslog messages. SAOS can act as a Syslog originator using TLS transport in the client role.

To use syslog over TLS, the Syslog originator (the SAOS device) and collector must be configured with signed device certificates and private keys. They can be preconfigured with the CA certificate (chain) that signed the device certificate.

The secure collectors hostname or IP is configured on the SAOS switch as a Syslog TLS collector. To send a Syslog message, the SAOS switch initiates a TLS connection to the collector. The two endpoints perform configured authentication and establish a TLS connection. Syslog messages are then transmitted by means of the TLS connection, as shown in this figure.

Figure 11-2
Syslog by means of TLS



RFC 5425 also includes a number of mechanisms for authentication and authorization that must be supported:

- End-entity certificate based authorization (fingerprint checking)
- Certificate path validation (checking certificate against trusted CA/CRLs)
- Subject Name Authorization (checking certificate fields against locally configured peer dns name or ip address)

Although support for these mechanisms is required, the user can enable or disable any or all of them according to their security needs and the collector configuration. Note that RFC 5425 allows unauthenticated operation of either the transport sender or receiver or both. Unauthenticated operation it is not recommended.

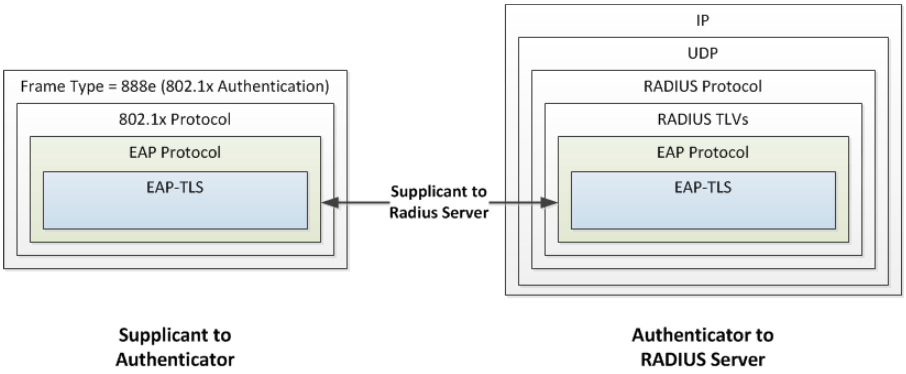
Secure Syslog procedures are:

- “Enabling Syslog TLS” on page 11-27
- “Configuring peer certificate re-authentication for syslog collectors” on page 11-30

EAP-TLS

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is an Internet Engineering Task Force (IETF) open standard that uses the TLS protocol for authentication. EAP-TLS messages are carried inside EAP messages carried in 802.1x frames or RADIUS UDP packets as shown in this figure.

Figure 11-3
EAP-TLS messages


Frame Type = 888e (802.1x Authentication)
802.1x Protocol
EAP Protocol
EAP-TLS
Supplicant to Radius Server
IP
UDP
RADIUS Protocol
RADIUS TLVs
EAP Protocol
EAP-TLS
Supplicant to Authenticator
Authenticator to RADIUS Server

EAP-TLS provides a significantly higher level of security than EAP-MD5. EAP-MD5 uses a weak password hash and only provides authentication of the EAP peer to the EAP server, but no mutual authentication. As a result EAP-MD5 is vulnerable to attacks. EAP-TLS uses X.509 certificates to authenticate the supplicant. The supplicant can optionally verify the identity of the authentication/RADIUS server.

X.509 certificates

X.509 certificates contain owner information, a public key, and a signature which prove that the certificate was approved by a higher level certificate authority. They may also contain additional information which includes limitations on what the certificate can be used for and a valid date range.

End entities also require a private key to establish identity since it is paired with a public key in its certificate. Private keys are protected by encryption with a passphrase. This means that the key is useless without the passphrase, providing that the passphrase is protected.

When a client wants to prove its identity to a server, the signed, public device certificate and private device key/passphrase must previously be installed on the client, and the root certificate that signed the client's certificate must be installed on the server. Intermediate certificates can be bundled with the root certificate on the server or with the device certificate on the client. During authentication, the client provides its device certificate to the server and uses its own private key to prove ownership of that certificate. The server verifies the certificate's signature against a chain of certificates back to the root certificate it holds and trusts.

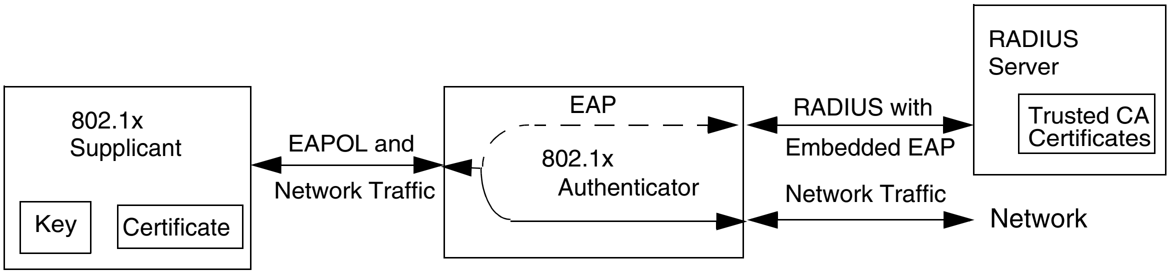
Authentication can be done in the opposite direction providing that the server has its own signed device certificate and private key and that the client has a copy of the root certificate that signed it. This can be the same root certificate that signed the client's device certificate or a different root certificate.

Authenticating EAP-TLS supplicant use case

In 802.1x, EAP-TLS is the supplicant and must have a device certificate and private key/passphrase installed. The server is the RADIUS server. It must have a copy of the root certificate. Intermediate certificates are omitted for simplicity.

The Certificate configuration for supplicant authentication figure describes the authentication of the EAP-TLS supplicant. During authentication, the supplicant presents its device certificate to the server which validates it against its store of trusted certificate authority (CA) certificates and optionally CRLs.

Figure 11-4
Certificate configuration for supplicant authentication

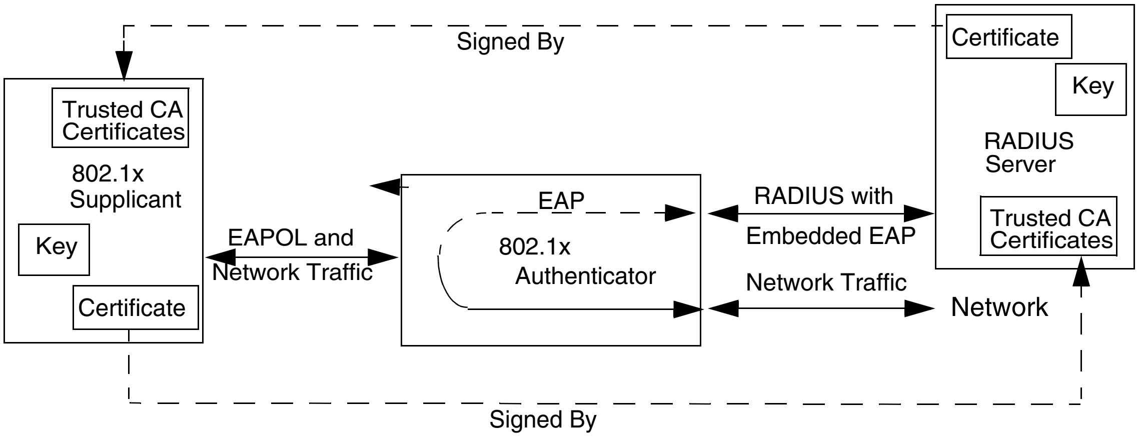


Supplicant EAP-TLS mutual authentication use case

If the supplicant is required to authenticate the server, the server must have a private key/passphrase and signed certificate. The supplication must also have a copy of the root certificate that signed it. During mutual authentication, the supplicant and server exchange their device certificates and each validates the other's against its trusted CA certificates and optionally a CRLs.

This figure describes how NTE authenticates the server.

Figure 11-5
Supplicant EAP-TLS mutual authentication



In the example, the RADIUS server provides its device certificate to the supplicant and uses its private key to prove ownership of the certificate. The supplicant verifies the certificate's signature against the chain of certificates back to the root certificate it holds and trusts.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies and procedures required to create, manage, distribute, use, store and revoke digital certificates.

PKI requires a public key and a private key (which must remain secret). The keys are linked so that messages encrypted with either of these keys can only be decrypted with the other.

PKI and X.509 provide the infrastructure that is used by 802.1x, and both are used for authentication and encryption.

The public key can be used to create messages that can only be decrypted by the owner of the private key. The owner of the private key is the only one who can create messages that can be decrypted with the public key. The public key can be used to verify the identify of the private key owner and to communicate securely with the private key owner. Private keys are encrypted with a passphrase that must be presented each time the key is used for any purpose.

SAOS provides the ability to install CA certificates, certificate revocation lists (CRLs), device certificates, and device private keys with passphrases. These are stored in non-volatile memory. Private keys and their passphrases cannot be readable from outside.

During installation, SAOS performs basic checks on the certificates to verify that they are actual certificates in readable formats, and that the passphrase can correctly decrypt the private key. SAOS provides basic display functionality for certificates, and is able to verify the presence of the private key.

Trusted CA certificates are stored globally for use by any application or port since the infrastructure checks device certificates against any trusted certificate in a CA directory. Device certificates and private keys are stored on a per application/port basis since different applications/ports may require certificates signed by different CAs.

Trusted CAs, CRLs, device certificates and private keys are pre-installed. Users can install or update these by commands that instruct SAOS to get them from an xFTP or HTTP server. Updated information can be reinstalled at any time.

X.509

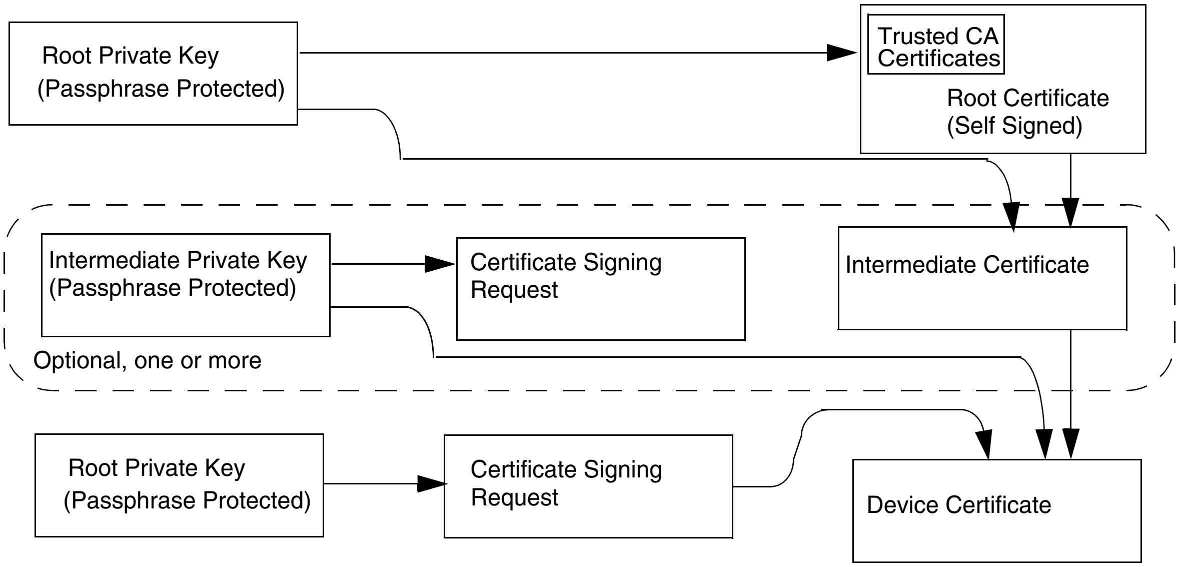
X.509 is an ITU-T standard for PKI. X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. PKI and X.509 provide the infrastructure that is used by 802.1x, and both are used for authentication and encryption.

X.509 provides standards for encapsulating public keys in certificates and certificate revocation lists, and the certification path validation algorithm. Certificates contain additional information to identify the owner of the associated private key, use restrictions, such as validity date range, and a digital signature.

Certificates are signed with a private key. They may be self-signed or signed by a more trusted private key owner using their private key.

This figure shows an example of the relationship between private keys and device certificates, and certificate signing requests used to create certificates signed by a higher level certificate/owner.

Figure 11-6
Example relationship



Example use cases for PKI and X.509

This section outlines these use cases:

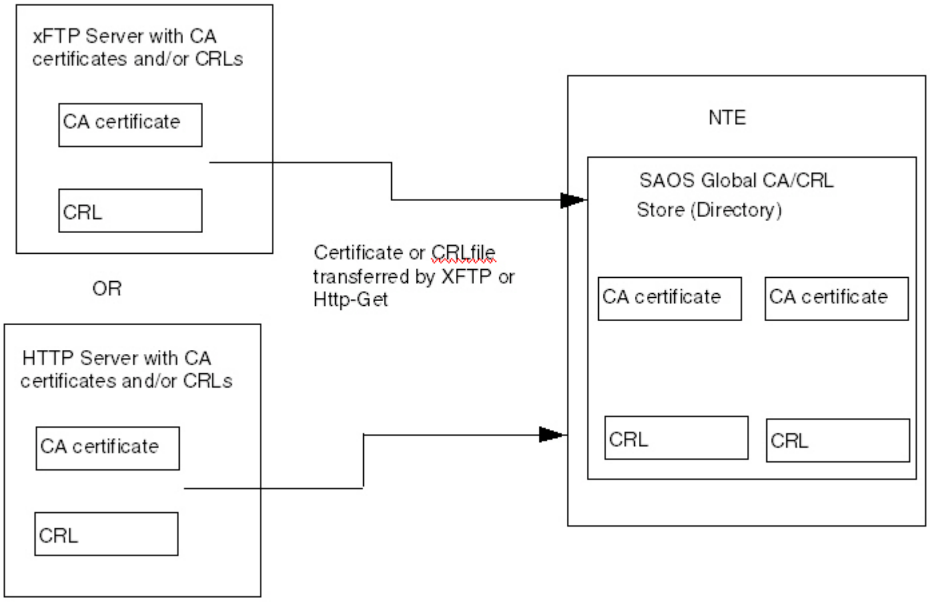
- “Certificate authority or certificate revocation lists installation” on page 11-14
- “Device certificate and private key installation” on page 11-15
- “NTE authenticated by server” on page 11-16
- “NTE authenticates another device” on page 11-16

Certificate authority or certificate revocation lists installation

xFTP commands are used to get the certificates from an xFTP server and install them in a global CA directory. These installed certificates can be used to verify a device certificate. CAs can also be installed from a web server by executing a SAOS command that takes a URL and does an HTTP-Get to install them in the same global CA directory. CRL files are handled in the same manner and installed in the same directory. Applications requesting OpenSSL to validate a device certificate can specify this directory as the ca_path and OpenSSL does everything else.

This figure shows the installation of a CA certificate or CRLs.

Figure 11-7
CA certificate or CRL installation


xFTP Server with CA certificates and/or CRLs
CA certificate
CRL
OR
HTTP Server with CA certificates and/or CRLs
CA certificate
CRL
Certificate or CRLfile transferred by XFTP or Http-Get
NTE
SAOS Global CA/CRL Store (Directory)
CA certificate
CA certificate
CRL
CRL

Device certificate and private key installation

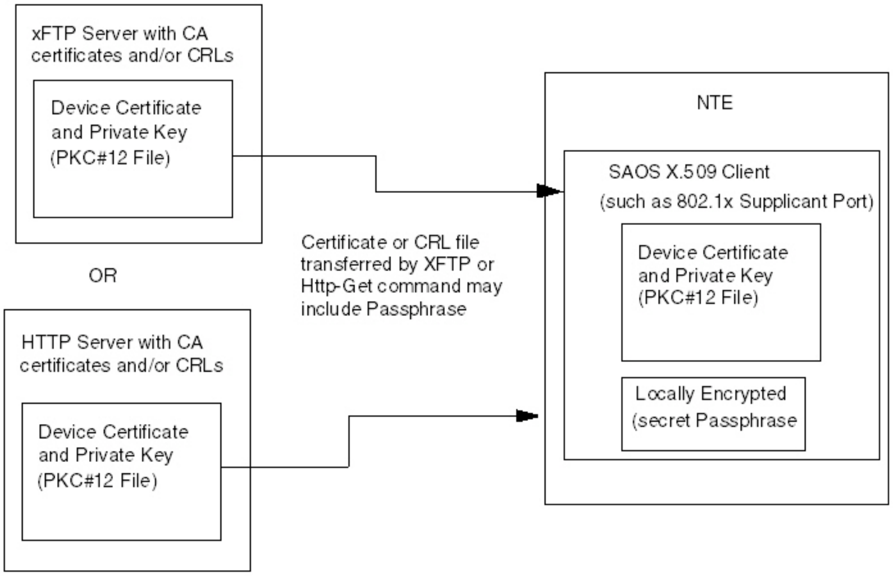
Device certificates and their associated private keys must be created and signed outside SAOS. These are bundled into a PKCS#12 file, which is the standard format for combining private keys, device certificates and optional intermediate certificates. PKCS#12 provides FIPS 140-2 compliant passphrase protection on private keys. External tools, such as OpenSSL, provide a mechanism to convert other formats and bundle keys and certificates into PKCS#12 format before installing them in SAOS.

To install device certificates and private keys, xFTP commands can be used to get the certificate files from an xFTP server and install them for a specific application and/or port. Device certificates can be installed from a web server by executing a SAOS command that takes a URL and does an HTTP-Get to install them in the same global CA directory.

If a file is passphrase protected (recommended), the passphrase can be specified as an optional part of the install command. The passphrase is locally encrypted and saved with the device certificate and private key file.

This figure shows the installation of a device certificate and private key.

Figure 11-8
Device certificate and private key installation


xFTP Server with CA certificates and/or CRLs
Device Certificate and Private Key (PKC#12 File)
OR
HTTP Server with CA certificates and/or CRLs
Device Certificate and Private Key (PKC#12 File)
Certificate or CRL file transferred by XFTP or Http-Get command may include Passphrase
NTE
SAOS X.509 Client (such as 802.1x Supplicant Port)
Device Certificate and Private Key (PKC#12 File)
Locally Encrypted (secret Passphrase

NTE authenticated by server

When the NTE wants to prove its identify to a server, the signed, public device certificate and the private device key/passphrase must previously be installed on the client. The root certificate that signed the client’s certificate must also be installed on the server. Intermediate certificates can be bundled with the root certificate on the server or with the device certificate on the client.

In 802.1x EAP-TLS, the NTE/client is the supplicant and must have a device certificate and private key/passphrase installed. The server is the RADIUS server and must have a copy of the root certificate.

During authentication, the client provides its device certificate to the server and uses its private key to prove ownership of the certificate. The server verifies the certificate’s signature against the chain of certificates back to the root certificate that it holds and trusts.

NTE authenticates another device

Authentication can be done in the opposite direction providing that the server has its own signed device certificate and private key. NTE must also have a copy of the root certificate that signed it. This may be the same root certificate that signed the client’s device certificate or a different root certificate. In 802.1x EAP-TLS mutual authentication, the supplicant is the NTE and it must verify the identify of the RADIUS server.

The RADIUS server provides its device certificate to the supplicant and uses its private key to prove ownership of the certificate. the supplicant verifies the certificate's signature against the chain of certificates back to the root certificate it holds and trusts.

Procedures for EAP-TLS are:

- "Configuring the 802.1x supplicant for EAP-TLS" on page 10-79
- "Displaying CA certificates" on page 10-83
- "Installing a trusted CA certificate" on page 10-84
- "Installing certificate revocation lists" on page 10-86
- "Displaying certificate revocation lists" on page 10-89
- "Configuring and displaying supplicant device certificates on a port" on page 10-90
- "Displaying supplicant information for a port" on page 10-91

OCSP

SAOS switches provide an Online Certificate Status Protocol (OCSP) client for use with X.509 authentication. This provides an optional real time check of peer certificate revocation status by querying an external OCSP responder over HTTP. The SAOS switch attempts to contact responders using OCSP URLs contained in the certificate and/or a user configured default responder URL. Responders are queried one at a time until a response indicates that the certificate is either valid or revoked. If no server responds with a status of valid, the authentication fails.

SSH Authentication

Normal password authentication is enabled by default. Additional authentication methods can be configured.

Public/Private key authentication

SSH supports public key based authentication. In public key based authentication, a password is not required. Instead, a key pair consisting of a private key and a public key is generated, then encrypted and stored on the server. The private key must be distributed to the client machine.

With public and private keys properly installed, the user can perform sftp file transfers or ssh to an external server with no password. In this scenario, the private key on the client acts as a complex password that is never transmitted over the wire. Instead, the server generates random data, encrypts it with the public key and sends it to the client. The client decrypts this message with its private key and sends the original data back to the server, thereby proving possession of the private key.

Since the private key grants the same access as a password, it must be protected just as a password is. When the key pair is generated, the private key can be optionally protected with a passphrase. This encrypts the private key. When accessing a server using a passphrase protected private key, the client requests the passphrase.

> ***Note:*** SSH can be configured to require both a password AND a private key (which can, in turn, require a passphrase for use). SAOS provides configuration to enable/disable this ability. As this can easily lead to locking out all users if public keys are not present, particularly since this setting is part of the configuration file, this setting is only applied to accounts that have public keys installed. It is still the user's responsibility to provide proper public keys, and maintain/protect the matching private keys.

SSH with X.509 authentication

RFC 6187 allows for X.509 certificates to be used to authenticate users. This is similar to the approach used for SSH public key authentication but it uses X.509 certificates instead of public keys to verify the identity on both the client and the server. After the certificates are exchanged, they are validated against a certificate authority (CA) certificate and against optional certificate revocation lists (CRLs). If this validation is successful, an optional Online Certificate Status Protocol (OCSP) validation can be done. If the peer certificate passes all validation, a connection is established. In SAOS switches, this is done using OpenSSH with PKIX-SSH.

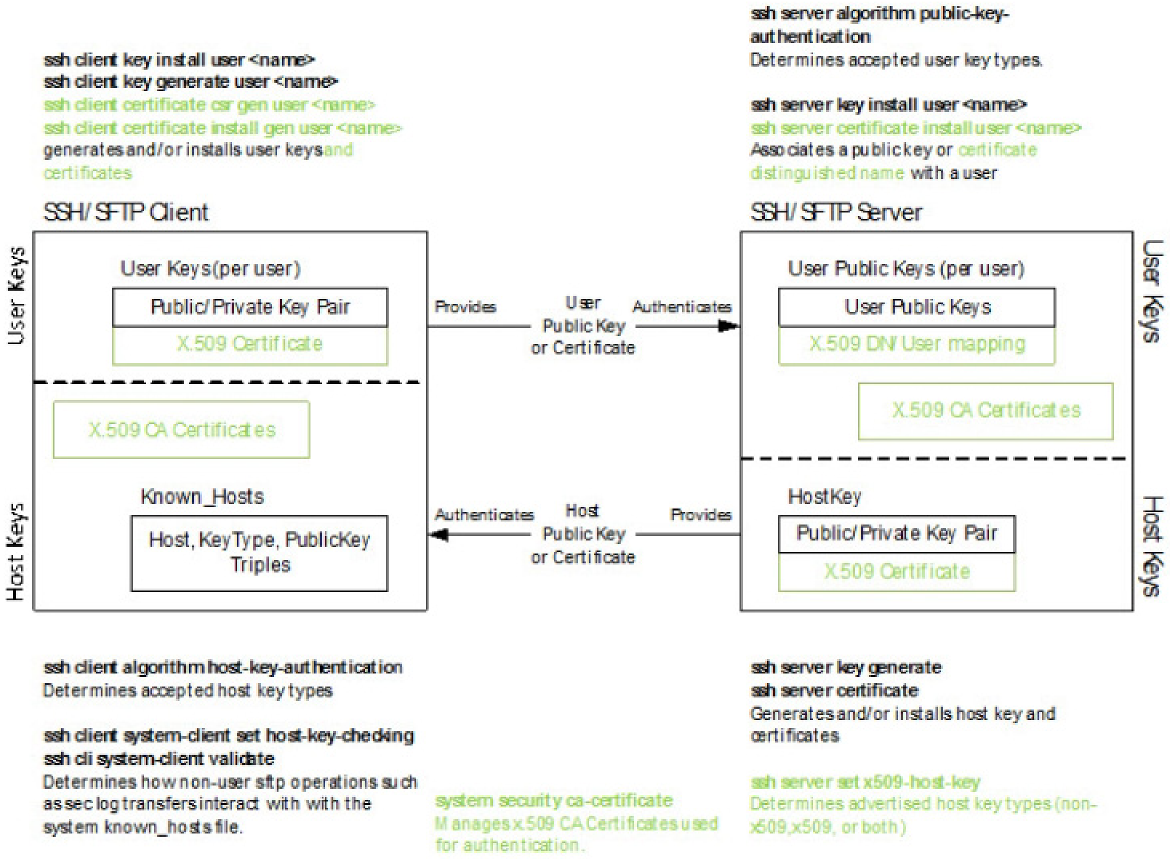
If X.509 authentication is enabled and no CA is installed, then authentication fails and an alternate method is needed to manage the device to recover. For example, if X.509 is enabled on an SAOS switch without a CA installed, then attempts to login to the 8700 switch fail until either a correct CA is installed or X.509 is disabled.

> ***Note:*** This is only possible if the server remains at the default settings.

In summary, SSH configuration is essentially separated into four parts (see SSH Configuration—items shown in green indicate optional X.509 configuration):

- Server Host Key configuration
- Server User Key configuration
- Client Host Key configuration
- Client User Key configuration

Figure 11-9
SSH Configuration


ssh client key install user <name>
ssh client key generate user <name>
ssh client certificate csr gen user <name>
ssh client certificate install gen user <name>
generates and/or installs user keys and certificates
ssh server algorithm public-key-authentication
Determines accepted user key types.
ssh server key install user <name>
ssh server certificate install user <name>
Associates a public key or certificate distinguished name with a user
SSH/SFTP Client
SSH/SFTP Server
User Keys
User Keys (per user)
Public/Private Key Pair
X.509 Certificate
Provides
User Public Key or Certificate
Authenticates
User Public Keys (per user)
User Public Keys
X.509 DN/User mapping
User Keys
X.509 CA Certificates
X.509 CA Certificates
Known_Hosts
Host, KeyType, PublicKey Triples
Authenticates
Host Public Key or Certificate
Provides
HostKey
Public/Private Key Pair
X.509 Certificate
Host Keys
Host Keys
ssh client algorithm host-key-authentication
Determines accepted host key types
ssh client system-client set host-key-checking
ssh cli system-client validate
Determines how non-user sftp operations such as sec log transfers interact with with the system known_hosts file.
system security ca-certificate
Manages x.509 CA Certificates used for authentication.
ssh server key generate
ssh server certificate
Generates and/or installs host key and certificates
ssh server set x509-host-key
Determines advertised host key types (non-x509, x509, or both)

Procedure 11-1
Displaying the security configuration

Display the security configuration.

Step **Action**

1 Display the security configuration:

```
system security show
```

—end—

Example

This example shows the output for the system security show command:

```
> system security show

+------------ SYSTEM SECURITY -------------+
| Setting     | Admin State    | Oper State  |
+-------------+----------------+-------------+
| Security    | enhanced       | enhanced    |
| Encryption  | normal         |             |
| Signing     | disabled       | disabled    |
+-------------+----------------+-------------+
```

Procedure 11-2
Configuring the encryption mode

You can

- set the security mode to FIPS
- set the security mode to normal

Step **Action**

1 Configure the encryption mode:

```
system security set {encryption-mode <fips | normal>}
```

where

encryption-mode <fips | normal> sets the encryption mode to FIPS or normal.

2 Restart the switch.

—end—

Example

This example shows the output for setting the encryption mode to FIPs:

```
> system security set encryption-mode fips-140-2
WARNING: Change to fips-140-2 encryption mode will not take effect
         until the next system restart!

> system security show

+------------ SYSTEM SECURITY -------------+
| Setting     | Admin State    | Oper State   |
+-------------+----------------+-------------+
| Security    | enhanced       | enhanced     |
| Encryption  | fips-140-2     | fips-140-2   |
| Signing     | disabled       | disabled     |
+-------------+----------------+-------------+
```

Procedure 11-3
Setting the security mode

Set the security mode to normal or enhanced security mode. Set the security mode to enhanced security if you need to run the device in a JITC-compliant environment.

> **WARNING**
> **Enhanced Security Mode**
> Enhanced security mode is only required if you need to run a device in a JITC-compliant environment. Do not put a device in enhanced security mode if this is not required. Operate devices in normal mode for non-JITC operations.

Setting the enhanced security mode on the device resets the device to factory defaults. A reset to factory defaults does not change the enhanced security mode setting.

You must have super user privileges to perform this procedure.

Step Action

1 Set the security mode:

```
system security set security-mode <enhanced|normal>
```

—end—

Example

This example sets the device security mode to enhanced.

```
> system security set mode enhanced
WARNING: Setting enhanced security mode requires a reset to factory defaults.
   System will be restarted: All configuration will be lost!
   You cannot abort this operation once it has begun.

Proceeding in 5 seconds. Press <CTRL> C to abort...
```

Procedure 11-4
Enabling and disabling NTP authentication

By default, NTP authentication is disabled for the NTP client.

Step **Action**

To enable NTP authentication:

1 Enable NTP authentication:

```
ntp authentication enable
```

To disable NTP authentication:

2 Disable NTP configuration:

```
ntp authentication disable
```

—end—

Procedure 11-5
Adding keys

You can add up to 32 MD5 keys. The key ID is a U32 value between 1 and 65534. If a key ID is entered or displayed as 0, this value implies there is no key. The MD5 key is a 1 to 31 ASCII character string, and cannot be any of these characters:

- Space ( )
- Double quote (“)
- Number sign (#)
- TAB (\t)
- Return (\n)
- \0

There are three ways to add a key:

- **Plain text** - Entered directly.
- **Encrypted key** - Enter a key from an MD5 encrypted key generator.
- **Import from a key file** - Transfer a simple tag readable format file to the system and then import keys from it.

An example of simple tag readable format is:

KEY=11 MD5="myKey11"

KEY=266 MD5="myKey266"

When you add an MD5 key, regardless of the method, the key is saved in the configuration file as if it had been added as an encrypted key.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! NTP CLIENT CONFIG:
!
ntp authentication enable
ntp authentication key-id 1 md5 3bf313a5
ntp authentication key-id 11 md5 1def01f15eef65
ntp authentication key-id 266 md5 1def01f15eec6214
ntp add server 192.83.249.31
ntp add server 132.236.56.250
!
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Step	Action

To add an MD5 key in plain text

1 Add an MD5 key in plain text:

```
ntp authentication add key-id <NUMBER> md5 <MD5AuthKey>
```

To add an MD5 key in encrypted form

2 Add an MD5 key in encrypted form:

```
ntp authentication add key-id <NUMBER> md5
<MD5AuthKeyEncrypt>
```

To import an MD5 key from a file

3 Import an MD5 key from a file:

```
ntp authentication import filename <FileName>
```

To remove an MD5 key

4 Remove an MD5 key:

```
ntp authentication remove key-id <NUMBER>
```

Example

These examples show how to add and remove MD5 keys.

Add an MD5 key in plain text.

```
> ntp authentication add key-id 1 md5 Key1
```

Add an MD5 key in encrypted form

```
> ntp authentication add key-id 1 md5 3bf313a5
```

Import an MD5 key from a file

```
> tget 192.168.41.68 ntp_simple_tag.key ntp_simple_tag.key
Received 46 bytes in 0.0 seconds.
Received 2000 bytes/second.
> ntp authentication import filename ntp_simple_tag.key
```

Remove an MD5 key

```
> ntp authentication remove key-id 1
```

Procedure 11-6
Enabling and disabling software signature checking

Software signature checking must be enabled for software loads to be validated. Software signing can be enabled or disabled by users with super privileges.

> ***Note:*** Software signature checking is disabled by default.

Step	**Action**
1	Enable software signature checking: `system security set software-signing-mode <on|off>`

—end—

Procedure 11-7
Enabling Syslog TLS

To use Syslog TLS, a private key must be created and an X.509 certificate must be signed and installed.

> ***Note:*** Syslog TLS is enabled by default. Syslog collectors are also enabled by default after they are added.

Step	**Action**

1 Install a device certificate (see "Creating and installing device certificates" on page 9-23).

2 Configure syslog tls to use that certificate, giving it the cert-name used when creating/installing the device certificate:

```
syslog tls set cert-name <cert-name>
```

3 Verify the syslog tls certificate:

```
syslog tls show certificate
```

4 (Optional) Add a Syslog TLS collector.

a. Create the syslog tls collector:

```
syslog tls create collector <IP address or host name>
```

b. Verify Syslog TLS connection to the collector.

```
syslog send msg <String[1..128]> severity <String>
```

This causes a Syslog message to be sent to the collector.

c. Verify that the collector received the message.

d. (Optional) Enable or disable Syslog TLS checking the configured collector's hostname or IP address against the Subject Common Name or Subject Alternative Name fields in the collectors certificate:

```
syslog tls set check-ip-host on|off
```

e. (Optional) Configure a different reference identifier than the configured collector's hostname when checking Subject Common Name or Subject Alternative Name:

```
syslog tls set collector <IP address or host name>
trusted-dns <fully-qualified-domain-name>
```

Note: This is useful when the collector is specified by IP address but the certificate contains a domain name.

5 (Optional) Enable or disable ciphersuites:

```
syslog tls algorithm cipher-suite enable|disable cipher-
suite <String>
```

Example

```
> syslog tls set cert-name test

> syslog tls show certificate

+----------------- SYSLOG TLS DEVICE CERTIFICATE ----------------+
| Parameter            | Value                                    |
+----------------------+------------------------------------------+
| Certificate Name     | test                                     |
+----------------------+------------------------------------------+
| Private Key          | Present                                  |
| Key Type             | RSA (2048)                               |
+----------------------+------------------------------------------+
| Device Certificate   |                                          |
|  Subject Common Name | SaosCertificate                          |
|  Issuer Common Name  | MyCA                                     |
|  Valid To            | Oct  5 15:02:01 2018 GMT (11 months)     |
+----------------------+------------------------------------------+
```

This example adds and tests a syslog collector.

```
> syslog tls create collector 10.10.10.10
> syslog send msg "testing 1 2 3" severity emergency
```

This example configures Syslog TLS to check the configured collector's hostname or IP address against the Subject Common Name or Subject Alternative Name fields in the collectors certificate.

```
syslog tls set check-ip-host on
```

This example configures a different reference identifier than the configured collector's hostname when checking Subject Common Name or Subject Alternative Name.

```
> syslog tls set collector 10.10.10.10 trusted-dns <fully-qualified-domain-
name>
```

This example enables and disables ciphersuites.

```
> syslog tls algorithm cipher-suite enable cipher-suite
TLS_RSA_WITH_AES_128_CBC_SHA
> syslog tls algorithm cipher-suite disable cipher-suite
TLS_RSA_WITH_RC4_128_MD5
```

Procedure 11-8
Configuring Syslog TLS OCSP client

OCSP can be enabled to do real time certificate status checks when validating a Syslog TLS collector's X.509 certificate.

Step **Action**

1 Enable or disable OCSP checking:

```
syslog tls ocsp enable|disable
```

2 Set OCSP default responder.

```
syslog tls ocsp set default-responder http://<String>
```

3 (Optional) Set OCSP responder first attempt preference.

```
syslog tls ocsp set responder-preference http://<String>
```

4 Display the server statistics to debug issues with the Syslog TLS connection to the collector.

```
syslog tls show collector <IP Address> statistics
```

Example

This example configures an Syslog TLS OCSP client.

```
> syslog tls ocsp enable
> syslog tls ocsp set default-responder http://10.1.1.100:8080
> syslog tls ocsp enable
> syslog tls ocsp set responder-preference http://10.1.1.100:8080
> syslog tls show collector 10.10.10.10 statistics

+------------------- SYSLOGTLS COLLECTOR 1 STATISTICS ----------------+
| IP Address             | 10.10.10.10                               |
| Hostname               | 10.10.10.10                               |
+------------------------+-------------------------------------------+
| Connection Attempts    | 1                                         |
| Successful Connections | 0                                         |
| Failed TCP Connections | 0                                         |
| Failed TLS Connections | 1                                         |
| Timed Out Connections  | 0                                         |
| Unexpected Closes      | 0                                         |
| Closed Connections     | 0                                         |
+------------------------+-------------------------------------------+
| Last Transport Error   | X509 verification error : unable to get   |
|                        |   local issuer certificate                |
+------------------------+-------------------------------------------+
| Overflow Msgs Dropped  | 0                                         |
+------------------------+-------------------------------------------+
```

Procedure 11-9
Configuring peer certificate re-authentication for syslog collectors

Configure peer certificate re-authentication for syslog collectors as required by the network plan.

You must have administrative privileges to perform this procedure.

Step **Action**

1 Enable SSH client peer re-authentication:

```
syslog tls peer-cert-reauth enable
```

2 Set the re-authentication period

```
syslog tls peer-cert-reauth set {[period
<duration>][ocsp-multiplier <NUMBER: 0..50>]}
```

where

period duration	Sets the re-authentication period. The default is 1 hr).
ocsp-multiplier	defines the period between doing OCSP when re-authentication (OCSP period = re-authentication period * ocsp-multiplier.) The default is 24hr.

3 Display peer certificate re-authentication attributes:

```
syslog tls peer-cert-reauth show
```

—end—

Procedure 11-10
Displaying the NTP authentication configuration

Display the NTP authentication configuration to verify the configuration.

Step	Action
1	Display an MD5 key: `ntp authentication show`

Example

This example shows sample output for the MD5 authentication show command.

```
> ntp authentication show

+------------------- NTP CLIENT STATE -------------------+
| Parameter               | Value                        |
+-------------------------+------------------------------+
| Admin State             | Enabled                      |
| Auth Admin State        | Disabled                     |
| Mode                    | Polling                      |
| Polling Interval (min)  | 16                           |
| Polling Interval (max)  | 16                           |
| Config State            | user                         |
| DHCP NTP Option State   | On                           |
| Sync Notification       | Off                          |
| Delay  (ms)             | 0.000                        |
| Offset (ms)             | 0.000                        |
| Jitter (ms)             | 0.000                        |
| Drift  (ppm)            | 0.000                        |
| Synchronized            | False                        |
+-------------------------+------------------------------+

+-------------------------------- NTP MD5 AUTH KEYS -----------------------+
| Key ID      | MD5 (Encrypted Value)                                       |
+-------------+-------------------------------------------------------------+
| NO KEYS                                                                   |
+-------------+-------------------------------------------------------------+

+--------------------------- NTP SERVER CONFIGURATION ---------------------------------------------------+
|                      |                | Auth   |  Config   |Admin|Oper |Server| Server  |Auth | Offset |
| IP Address           | Host Name      | Key ID |  State    |State|State|State |Condition|State| (ms)   |
+----------------------+----------------+--------+-----------+-----+-----+------+---------+-----+--------+
| No Servers           |                |        |           |     |     |      |         |     |        |
+----------------------+----------------+--------+-----------+-----+-----+------+---------+-----+--------+
```

Security log

The security log contains records of login/logout activity and other security-related events specified by the system's audit policy. The security log is used by administrators to detect and investigate attempted and unsuccessful authorized activity. All events are recorded in real time by default.

The device has a limited-size log. Old entries are discarded to make room for new entries. Any discarded information can be uploaded to a management station before it is discarded so that nothing is lost, provided that there is connectivity to the management station. A periodic full log upload may be scheduled to ensure that the management station is relatively up to date.

Security log access

Security logs can only be accessed by users with super user privileges. These users are administrators, and only they can clear the security log. When the log is cleared, one log entry is created in the freshly cleared log indicating the time it was cleared and the administrator who cleared it.

The security log cannot be edited to delete or add specific events.

Only administrators can copy, offload, and back up the security log. This means that when users create a state dump, the security log is only included in the state dump if the user has super user privileges.

Administrative actions are recorded in a security log. This recording cannot be disabled.

The security log contains a record of events defined by Ciena. Administrators can disable some of these events if they choose, but cannot add events to the log. Dynamic control of the types of events recorded include selective disabling of the recording of default audit events and the inclusion of other events such as:

- the inclusion of other events such as valid user authentication attempts
- the creation and deletion of network resources
- changes in network configuration
- changes in security states of users, services, and nodes

Security log audit entries

The events that can be logged include:

- Account access events
- Account management — adding, deleting, changing user accounts and passwords
- Policy changes — changes to the auditing policy
- Directory service access
- Object/resource access
- Privilege use
- Process tracking
- System events

Auditing account management

The accounts in the network device are privileged or system-level accounts. Therefore, account management is vital to the security of the network device. Account management by an administrator ensures access to the network device is being controlled securely by granting access to only authorized personnel with the appropriate and necessary privileges. Auditing account modification along with an automatic notification provides the necessary reconciliation that account management procedures are being followed. If modifications to management accounts are not audited, reconciliation of account management procedures cannot be tracked.

The DoD defines the list of events that a device must provide for an audit record generation:

- Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information such as classifications levels
- Access actions, such as
    - successful and unsuccessful logon attempts
    - privileged activities or other system level access
    - starting and ending time for user access to the system
    - concurrent log ons from different workstations
    - successful and unsuccessful accesses to objects
    - all program initiations
    - all direct access to the information
- All account creation, modification, disabling and termination actions

Mandatory security events

This section contains a list of the events that are mandatory and must be recorded. While other events that are logged in the security log are configurable, the events corresponding to the actions described in "Auditing account management" on page 12-2 are not:

- SecEvent_LoginAccepted
- SecEvent_SimulSessions
- SecEvent_TooManySessions
- SecEvent_Logout
- SecEvent_IntrusionDetection
- SecEvent_UserCreate
- SecEvent_UserDelete
- SecEvent_UserPrivSet
- SecEvent_UserAuthSet
- SecEvent_UserPasswordSet
- SecEvent_UserSecretSet
- SecEvent_UserPasswordClear
- SecEvent_MaxLimitedUsersSet
- SecEvent_MaxSuperUsersSet
- SecEvent_MaxAdminUsersSet
- SecEvent_MaxUserSessionSet
- SecEvent_MinPasswordUppercaseCharSet
- SecEvent_MinPasswordLowercaseCharSet
- SecEvent_MinPasswordNumericCharSet
- SecEvent_MinPasswordSpecialCharSet
- SecEvent_MinPasswordChangeCharSet
- SecEvent_MaxPasswordRunLengthSet
- SecEvent_DisallowUserNameSet
- SecEvent_DisallowDictWordsSet
- SecEvent_KillLogin
- LoggingEvent_SecLogCleared

An audit record contains the following information as applicable to the event:

- Login username
- Method of login (Telnet, SSH)

- IP address
- Privilege level (optional, but desired)
- Date and time
- Information to establish where the event occurred, such as
  - device hardware components
  - device software modules
  - session identifiers
  - filenames
  - host names
  - functionality
- Outcome of the event, as to whether an attack was successful or if changes were made to the security state of the system
- Full text recording of privileged commands

Auditing account login and logout

An audit record is made for each successful login/logout, whether the access method is SSH, Telnet or serial port.

Upon successfully logging in, the network device notifies the administrator of the date and time of the last login. The security log contains the number of successful/unsuccessful logins on any account.

Audit records are made for each unsuccessful login attempt. There is a maximum number of three attempts that can be made before the system closes the connection. If this number is reached and the connection is closed, a separate audit log for this event is generated.

The network device must notify the administrator of changes to access and/or privilege parameters of the administrator's account that occurred since the last log on.

Security log management

The local log holds 20,000 entries. It can be examined and it filters options like those in the command log. Entries in the local log may be viewed in local or UTC time zones. These entries are controlled by system timestamp setting. The size limit is the date range of the available log which depends on the activity level. The local log may be cleared. This clearing is logged. Any discarded information has usually been configured to be exported first. The local log is included in a state-dump if the user is privileged to access it.

The exported log is unlimited in size. If the exported log is trimmed, it is done by the external system. Entries are all in UTC so that logs of all systems may be correlated worldwide.

Log collection, rotation and backup

The security log provides a minimum number of entries. The system provides the ability by means of the CLI to offload the security log for storage and further analysis. The system also provides a way to back up security log onto a different system at least every seven days.

Log analysis, search and reporting

The user can analyze the log for specific content based on:

- Key words
- Event severity

Audit policy

The audit policy defines what is logged, the severity and the default.

Default audit policy

By default, the security log shall be enabled to record all events defined in the audit policy.

Configurable audit policy

Unauthorized personnel may be able to prevent the auditing of critical events as there is no capability to restrict which roles and individuals can select which events are audited. Misconfigured audits may make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Required notifications

This section outlines the notifications that are required.

Security log capacity

The audit mechanism notifies the administration when the audit log space is near capacity.

Security log failure

The network device alerts administrators in the event of an audit processing failure. Without this notification, administrators may be unaware of an impending failure of the audit capability and system operations may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Imminent attack notification

The device contains a real-time mechanism that monitors the occurrence or accumulation of security auditable events that may indicate an imminent security violation. This optional alarm can be turned on. It immediately notifies the administrator when administrator-defined thresholds are exceeded.The operator must configure the alarm threshold. If the occurrence or accumulation of these security relevant events continues, the device provides the capability to take the least disruptive action to terminate the event.

Procedure 12-1
Enabling and disabling specific events in the security log

You can enable or disable specific events in the security log.

You must have super user privileges to perform this procedure.

Step **Action**

1 Enable or disable specific events in the security log:

```
system security log <enable | disable> event-id <NUMBER>
```

where

event-id <NUMBER>	is the event-id that you wish to enable or disable system security logging for.

—end—

Procedure 12-2
Clearing system security logs and statistics

You can clear system security logs and/or statistics.

You must have super user privileges to perform this procedure.

Step	Action
1	Enable or disable system security logging: `system security log clear [statistics]`

—end—

Procedure 12-3
Configuring security log external transfers

You can configure security log transfers to enable the automatic transfer of security logs to an external server.

> ***Note:*** Enabling automatic log transfers limits the logs to users with super user privileges and above.

You can configure security log transfers from:

- FTP server
- TFTP server
- SFTP server

Step **Action**

To configure security log transfers from an FTP server

1 Configure security log transfers from an FTP server:

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

where

ftp-server <ip-host-str>	is the ftp-server name.
login-id <username>	is the FTP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

To configure security log transfers from a TFTP server

2 Configure security log transfers from a TFTP server:

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

where

tftp-server <ip-host-str>	is the tftp-server name.
login-id <username>	is the TFTP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

To configure security log transfers from an SFTP server

3 Configure security log transfers from an SFTP server:

```
system security log transfer set {sftp-server <ip-host-
str> [login-id <username> [<password-attr>|<echoless-
password-attr>][server-port <INTEGER: 1...65535>]}
```

where

sftp-server <ip-host-str>	is the sftp-server name.
login-id <username>	is the SFTP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

4 Configure the path on the external server:

```
system security log transfer set dest-path
<String[1..127]
```

where

dest-path <String[1..127]	is the destination path for the transfer.

5 Set the transfer interval:

```
system security log transfer set interval <duration>
```

where

interval <duration>	is the periodic transfer time.

6 Enable automatic security log transfers:

```
system security log transfer enable
```

—end—

Procedure 12-4
Configuring security log transfers

You can configure security log transfers.

You must have super user privileges to perform this procedure.

Step **Action**

1 Configure security log transfers:

```
system security log transfer set {[connection-timeout
<SECONDS: 1..100>] [dest-path <String[1..40>] [discards-
exported <on|off>][interval <duration: {N[yMwdhms]}* e.g.
1h10m3s>] [start-plus-or-minus <duration: {N[yMwdhms]}*
e.g. 1h10m3s>][retries <NUMBER: 1..10>][retry-interval
<SECONDS: 1-300>]

{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

connection-timeout <SECONDS: 1..100>
is the duration in seconds before retry times out.

dest-path <String[1..40]>
is the path on destination.

discards-exported <on|off>
turns on the automatic export of discarded log information.

interval <duration: {N[yMwdhms]}* e.g. 1h10m3s>]
is the maximum number of automatic uploads to occur.

start-plus-or-minus <duration: {N[yMwdhms]}* e.g. 1h10m3s>]
shift firs transfer time by up to (N[yMwdhms]..)

retries <NUMBER: 1..10>
is the maximum number of retries allowed.

where

retry-interval <SECONDS: 1-300>}	delay interval (in seconds) between retries
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 sftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password attr	collects the password interactively.
server-port <INTEGER: 1...65535	is the server-port number to connect to.

—end—

Example

This example configures security log transfers.

```
system security log transfer set interval 1h start-plus-
or-minus 15m
```

Procedure 12-5
Enabling or disabling automatic security log transfer

With a security log transfer, you can:

- enable system security log transfer automatically
- disable system security log transfer automatically

You must have super user privileges to perform this procedure.

Step	Action
1	Enable or disable security log transfer

```
system security log transfer <enable|disable>
```

—end—

Procedure 12-6
Transfer a security log manually

You can transfer a security log manually.

You must have super user privileges to perform this procedure.

Step	Action
1	Transfer a security log manually: `system security log transfer now`

—end—

Procedure 12-7
Displaying security log transfer settings

You can display security log transfer settings.

You must have super user privileges to perform this procedure.

Step **Action**

1 Display security log transfer settings:

```
system security log transfer show
```

—end—

Example

This example shows the output for the system security log transfer show command.

```
>system security log transfer show

+-------------- SYSTEM SECURITY LOG TRANSFER SETTINGS ----------------+
+-------------------------+-------------------------------------------+
| Export state            | Idle                                      |
| Export mode             | Disabled                                  |
| Export server           |                                           |
| Export username         |                                           |
| Export path             | ?                                         |
| Periodic export         | no                                        |
| Random staggered start  | no                                        |
| Export discards         | no                                        |
| Transfer timeout        | default                                   |
| Transfer retries        | 0                                         |
| Retry interval          | 0s                                        |
+-------------------------+-------------------------------------------+
```

Procedure 12-8
Displaying system security logs

You can display system security logs filtered by the parameters described in this table.

Table 12-1
Parameters for filtering security logs

Parameter	Description
containing	logs containing a specific string
from-date	entries from a specific UTC or local date
from-time	entries from a specific UTC or local time
last	recent entries into the command log
recent	entries into the history log in the last hour
since-activated	from system start of failover
tail	the latest entries
today	today’s entries in the command log
to-date	entries from a specified date
to-time	entries from a specific time
yesterday	yesterday’s entries in the command log
statistics	security log statistics
status	security log status

You must have super user privileges to perform this procedure.

Step Action

To display security logs containing a specific word

1 Display system security logs containing a specific word:

```
system security log show containing <STRING>
```

To display security logs from a specific date

2 Display system security logs from a specific date:

```
system security log show from-date <date: yyyy-mm-dd or
yy-mm-dd or mm-dd>
```

To display security logs from a specific time

3 Display system security logs from a specific time:

```
system security log show from-time <time: hh:mm:ss or
hh:mm>
```

To display recent security log entries into the command log

4 Display recent system security logs into the command log:

```
system security log show last <duration>
```

To display recent security logs in the last hour

5 Display recent security logs containing specific words:

```
system security log show recent containing <STRING>
```

6 Display the latest security logs:

```
system security log show tail <NUMBER>
```

7 Display security logs from a specific time:

```
system security log show to-time <time: hh:mm:ss or hh:mm>
```

To display all security logs

8 Display all security logs:

```
system security log show
```

To display security log statistics

9 Display security log statistics

```
system security log show statistics
```

To display security log status

10 Display security log status:

```
system security log show status
```

—end—

Example

This example shows output from the system security log show command when a specific word (Telnet) is specified.

```
> system security log show containing Telnet

11: August 25, 2015  14:37:30.391 [UTC] Sev:8 chassis(1): Telnet IP
10.128.233.1

50 User su:User 'su' successfully logged in from 10.128.233.150

12: August 25, 2015  20:03:03.359 [UTC] Sev:8 chassis(1): Telnet IP
10.128.233.1
```

```
50 User su:User 'su' logged out from 10.128.233.150 unexpectedly

13: August 26, 2015  13:43:26.060 [UTC] Sev:8 chassis(1): Telnet IP
10.128.233.1

05 User su:User 'su' successfully logged in from 10.128.233.105

14: August 26, 2015  18:41:52.564 [UTC] Sev:8 chassis(1): Telnet IP
10.128.233.1

05 User su:User 'su' logged out from 10.128.233.105 unexpectedly

16: August 26, 2015  18:42:35.465 [UTC] Sev:8 chassis(1): Telnet IP
10.128.233.1

05 User su:User 'su' successfully logged in from 10.128.233.105

--More--
```

This example shows output from the system security log show yesterday command.

```
> system security log show yesterday

38: August 31, 2015  12:17:27.472 [UTC] Sev:8 chassis(1): Telnet IP
10.128.235.1

67 User su:User 'su' successfully logged in from 10.128.235.167

39: August 31, 2015  20:34:07.305 [UTC] Sev:8 chassis(1): Telnet IP
10.128.235.1

67 User su:User 'su' logged out from 10.128.235.167
```

This example shows output from the system security log show statistics command.

```
> system security log show statistics

+------ SECURITY LOG STATISTICS ------+
|   Event ID  | Dis |           Count  |
+-------------+-----+------------------+
|    0x30013  |     |               1  |
|   0x1B0002  |     |               2  |
|   0x1B0003  |     |               1  |
+-------------+-----+------------------+
```

This example shows output from the system security log show status command.

```
> system security log show status

+-- SYSTEM SECURITY LOG STATUS --+
+-------------------+------------+
| Operational state | Enabled    |
| Transfers (auto)  | Disabled   |
+-------------------+------------+
```

Performing security containment and recovery

This section provides the procedures needed to perform security containment and recovery:

Procedure 13-1
Displaying user accounts

If your user ID has super or limited user access, you can display

- created users
- users who are currently logged on
- your own user name and access level

Step **Action**

To display all created users

1 Display all created users:

```
user show
```

To display users currently logged on to the device

2 Display all users currently logged on to the device:

```
user who
```

To display your user name and access level

3 Display your user name and access level:

```
user whoami
```

—end—

Examples

This example shows sample output for the user show command.

```
> user show

+----------------- USER ACCOUNT TABLE ---------------+
| Username                        | Privilege        |
+---------------------------------+------------------+
| New1                            | diag             |
| New2                            | super            |
| NewSuper                        | super            |
| admin                           | diag             |
| ann                             | super            |
| gss                             | diag             |
| marie                           | diag             |
| marie2                          | admin            |
| su                              | super            |
| user                            | limited          |
| user2                           | diag             |
+---------------------------------+------------------+

+---------------- USER ACCOUNT STATUS ---------------+
|                   | Max Network |  Current Active  |
| User Access Level |  Permitted  | Network | Serial |
+-------------------+-------------+---------+--------+
| Limited Users     |           5 |       0 |      0 |
| Admin Users       |           5 |       0 |      0 |
| Super Users       |           5 |       1 |      0 |
| Diag Users        |          12 |       0 |      0 |
| Total Users       |          12 |       1 |      0 |
+-------------------+-------------+---------+--------+

+--------------- USER ACCOUNT SETTINGS --------------+
| Setting                         | Value            |
+---------------------------------+------------------+
| Minimum Password Length         | 0                |
+---------------------------------+------------------+
```

This example shows sample output for the user who command.

```
> user who
+--------------------------------------- USER SUMMARY -------------------------+
| Username               |Idle Time|  Pid  | Terminal                          |
+------------------------+---------+-------+-----------------------------------+
| gss                    |     90m |  1025 | ttyS0                             |
| gss                    |      0m | 27889 | /telnet_[2001:db8:f018:1::1]      |
+------------------------+---------+-------+-----------------------------------+
```

This example shows sample output for the user whoami command.

```
> user whoami
username: su  access-level: super
```

Procedure 13-2
Displaying the Telnet server configuration

Display the Telnet server configuration when you want to view the Telnet server configuration.

Step	Action
1	Display the Telnet server configuration: `telnet server show`

—end—

Example

This example shows sample output for the telnet server show command.

```
> telnet server show

+--- TELNET GLOBAL CONFIGURATION ---+
| Parameter         | Value         |
+-------------------+---------------+
| Server            | Enabled       |
+-------------------+---------------+

+------- TELNET GLOBAL STATUS ------+
| Attribute            | Value      |
+----------------------+------------+
| Active Limited Users | 0          |
| Active Admin Users   | 0          |
| Active Super Users   | 1          |
| Active Diag Users    | 0          |
| Total Active Users   | 1          |
+----------------------+------------+
```

Procedure 13-3
Terminating a session

Terminate a session.

Step **Action**

To terminate user sessions

1 Terminate user sessions:

```
user kill pid <TAB>
```

To terminate all but your own session

2 Terminate all but your own session:

```
user kill all-but-me
```

—end—

Procedure 13-4
Changing a password for a user account

If a user password is forgotten, it cannot be retrieved. A superuser can assign the user a new password or the user can be deleted and added again with a different password.

Valid password characters comprise ASCII 32 (space) to ASCII 126 (tilde) with the exception of ASCII 34 (double quotes):

- If ASCII 32 (space) is used, the password string must be encapsulated by a pair of double quotes.
- If ASCII 32 (space) is used at the beginning or end of the password string, it is not considered part of the password and it is discarded.
- ASCII 34 (single double quotes character) is not allowed.

Further restrictions may be in place. See the procedure "Displaying the current user password policy settings" on page 8-15 to verify what current local restrictions may also apply.

Step **Action**

1 Change a password for a user account:

```
user set user <user> {access-level
<limited|admin|super|diag>} [echoless-password]
{nopassword}
```

where

user <user>	is the user account that you want to set a password for.
access-level <limited|admin | super|diag>	is the user access level.
echoless-password	collects user password interactively.
nopassword	no password.

—end—

Procedure 13-5
Deleting user accounts

Delete a user account when the account is no longer required.

Step	Action
1	Delete a user account:

```
user delete user <String[16]>
```

where

user <String[16]> is the user account to be deleted.

—end—

39XX/51XX Switches and Platforms

Administration and Security

SAOS 6.21.2
Publication: 009-3458-007
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**