Configuring Security on Avaya Virtual Services Platform 7000 Series

Release 10.3.2
NN47202-501
Issue 05.01
August 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides conceptual and procedural information you can use to configure security for Avaya Virtual Services Platform 7000 Series switches.

The security topics discussed in this document are provided with the following assumptions:

- You are familiar with networking concepts and terminology.
- You have basic knowledge of network topologies.
- You have experience with Graphical User Interface (GUI).
- You have experience with the following ACLI command modes:
  - User Executive
  - Privileged EXEC
  - Global configuration
  - Interface configuration
  - Router configuration

For detailed information about the ACLI command modes, see *Using ACLI and EDM on Avaya Virtual Services Platform 7000 Series*, NN47202–101.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Roadmap Reference for Avaya Virtual Services Platform 7000 Series*, NN47202–103.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
7D00080W	Avaya Stackable ERS and VSP Product Overview
7D00085V	Stackable ERS & VSP Installation, Configuration, and Maintenance
7D00085I	Stackable ERS & VSP Installation, Configuration, and Maintenance

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes,

downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this Release

The following sections detail what is new in this document for Avaya VSP 7000 Release 10.3 and Feature Pack Release 10.3.2.

Features

See the following sections for information about feature changes.

Multiple local RW and RO user accounts

Feature Pack Release 10.3.2 includes support for multiple local read-write (RW) and read-only (RO) user accounts on a switch. With this feature, up to 8 network administrators can be assigned an individual RW or RO user account. Multiple local RW and RO user accounts improves security by helping to avoid the use of shared accounts and makes user actions visible through the analysis of audit records.

For more information, see:

- Multiple local RW and RO user accounts_Concept on page 22
- ConfiguringMultipleLocalRW_ROuserAccts_ACLI on page 56
- Displaying local user information_ACLI on page 64

RO user password change in Priviledged EXEC

Feature Pack Release 10.3.2 includes support for RO users to change their account password in Privileged EXEC ACLI command mode.

For more information, see Changing the RO password on page 58.

Lockout for failed logon attempts

Feature Pack Release 10.3.2 includes support for the switch to deny a user password logon access after the maximum number of failed logon attempts is exceeded.

For more information, see:

- Configuring the failed logon attempt lockout interval on page 63
- Unlocking a locked-out user on page 63

Password expiration period

Beginning with Feature Pack Release 10.3.2, users can configure the period of time after which the password for Telnet or console access to the switch expires.

For more information, see Configuring password expiration period on page 60.

SNMP trap for port link status

Beginning with Feature Pack Release 10.3.2, you can configure the generation of a linkUp or linkDown SNMP trap for one or more switch ports.

For more information, see Configuring port link status trap generation on page 147.

RO user access to Telnet and SSH

Avaya VSP 7000 Series Release 10.3 supports read-only (RO) user permission to connect from the switch or Stack to another device using Telnet and Secure Shell (SSH) commands. In previous software releases, the Telnet and SSH commands required read-write (RW) user permission.

A secure agent image supports the capability to establish a SSH connection or Telnet session to another SSH or Telnet server device in the network using ACLI. A non-secure agent image supports Telnet sessions only.

With RO access, you can establish a SSH connection to another SSH server using DSA public key authentication, RSA public key authentication, or password authentication. With RO access, you can establish a Telnet connection to another Telnet server using password authentication.

For more information about how to establish an SSH connection, see Connecting SSH to a host on page 83 and SSH Client known hosts on page 37. For more information about how to establish a Telnet connection, see Connecting to a device using Telnet on page 81.

SSH RSA authentication

SSH RSA authentication provides increased security for Secure Shell (SSH) login. With this feature, the switch supports RSA public-private key encryption that uses a digital certificate. SSH RSA Authentication is supported when you select the RSA certificate option for a Secure Shell connection from a client PC to the switch.

For more information see:

- SSH service configuration on page 35 for conceptual information.
- Enabling or disabling SSH RSA authentication on page 84 for ACLI configuration.
- Downloading an SSH auth key on page 86 for ACLI configuration.
- Deleting an SSH RSA auth key on page 87 for ACLI configuration.
- Generating a new SSH RSA host key on page 89 for ACLI configuration.
- Deleting an SSH RSA host key on page 89 for ACLI configuration.
- Configuring SSH on page 123 for EDM configuration.

Limitations

When you download a new RSA key, the old RSA key is overwritten and you can no longer use the old RSA key to log on the switch.

Only one user can connect using an RSA public-private key-authentication. Multiple concurrent sessions for this unique user are possible.

Other changes

This section identifies document changes that are not related to new features.

TACACS+ configuration example

TACACS+ configuration example: Avaya Identity Engine Ignition Server on page 203 is added to the document.

SFP log and trap entries

Avaya VSP 7000 Series Release 10.3 adds log messages and SNMP trap entries when SFP devices are inserted or removed from a unit.

For more information, see SNMP trap support on page 26.

USB log and trap entries

Avaya VSP 7000 Series Release 10.3 adds log messages and SNMP trap entries when USB devices are inserted or removed from a unit.

For more information see SNMP trap support on page 26.

Chapter 3: Security fundamentals

This chapter provides conceptual information about the security features supported by the Avaya Virtual Services Platform 7000 Series to restrict access to your network.

Summary of security features

The tables in this section provide summary information about some of the security features available with the Avaya Virtual Services Platform 7000 Series.

Table 1: Password Authentication security

Password Authentication	Description
Description	Security feature.
What is being secured	User access to a switch or stack.
Layer	Not applicable.
Level of Security	Provides Read Only/Read Write access. The access rights are checked against Local Password.
Violations	Not applicable.
Configuring using interfaces	Console, ACLI, ASCII configuration file.
Restrictions and Limitations	Not applicable.

Table 2: IP Manager security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable or disable access for TELNET (Telnet On/Off), SNMP (SNMP On/Off), Secure Shell (SSH), and Web Page Access (Web On/Off) with or without a list of 50 IPv4 and 50 IPv6 addresses and masks. **Note:** The IPv6 parameter is valid only for switches that support IPv6.
What is being secured	User access to the switch through Telnet, SNMP, SSH, or Web.

IP Manager	Description
Per-Port or Per Switch	For each switch.
Layer	IP.
Level of Security	Access.
Violations	User is not allowed to access the switch.
Requirements for Setup	Optional IP Addresses or Masks, Individual Access (enable or disable) for TELNET, SNMP, SSH, or Web Page.
Configuring using interfaces	Console and ACLI.
Restrictions and Limitations	Not applicable.

IP Manager

You can limit access to the management features of the Avaya Virtual Services Platform 7000 Series by defining the IP addresses that are allowed access to the switch.

Important:

To avoid locking a user out of the switch, Avaya recommends that you configure ranges of IP addresses that are allowed to access the switch.

With IP Manager, you can do the following:

- Define a maximum of 50 IPv4 addresses, 50 IPv6 addresses, and masks that are allowed to access the switch. No other source IP addresses have management access to the switches.
- Enable or disable access to Telnet, SSH, SNMP, and Web.

Changes you make to the IP Manager list are reflected only after you restart the system. The sessions that were open at the time of configuring the IP Manager list remain unaffected.

The IP Manager list can check for SSH access to the switch.

User access limitations

Using ACLI, an administrator can limit user access by creating and maintaining passwords for Telnet and Console access. Password creation is a two-step process that requires first defining and then enabling the password.

You must be in the Global Configuration mode in ACLI to perform these tasks.

Note:

When you set a *username* and *password* to default, the change is only applied to the switch on which the command was run.

Password security

The Avaya Virtual Services Platform 7000 Series provides password security through a variety of mechanisms. The switch supports both default and customized user names and passwords for accessing a switch with read-only or read-write access, and it supports password security for SNMP access.

The following is a list of the types of password security provided by the switch:

- default switch read-only user name and password
- default switch read-write user name and password
- customized user names and passwords for read-only switch
- customized user names and passwords for read-write switch
- read-only community string (display limitation feature only)
- read-write community string (display limitation feature only)

Custom user names and passwords

The switch provides the ability to create custom user names and passwords for accessing the switch or stack. User names and passwords are created only by a user with read-write privileges.

Custom users and passwords cannot have specialized access conferred to them. Custom users have the same privileges as the default read-only or read-write access user. The read-only and read-write passwords cannot be the same.

Unified password authentication

With unified password authentication you can manage the local authentication type user name and password for a switch, whether the switch is part of a stack or a standalone unit.

For a stack environment, the local user name and password authentication is applied universally across all switches in a stack.

If you insert a standalone switch with authentication credentials and mode already configured into an existing stack, both authentication credentials and mode of stack base unit are applied to the newly inserted switch. This maintains unified authentication management throughout the stack.

If you remove a switch from a stack to have it function as a standalone unit, that switch retains the unified stack authentication credentials until you manually change the credentials.

Switch authentication is identical to stack authentication except when RADIUS or TACACS+ authentication is used for the stack and no IP address is configured for one or more of the stack units. In this case, the stack authentication type is set to RADIUS or TACACS+, the authentication type is automatically changed to “Local” for the units without IP addresses configured, and log messages are generated.

You can apply the following security methods to manage passwords for serial, Web, or Telnet access to a switch:

- local—uses the locally defined password
- none—disables the password
- RADIUS—uses RADIUS password authentication
- TACACS+—uses TACACS+ authentication, authorization, and accounting (AAA) services

Password length and valid characters

Valid passwords are between 10 and 15 characters long. The password must contain a minimum of the following:

- 2 lowercase letters
- 2 capital letters
- 2 numbers
- 2 special symbols. For example, !@#$%^&*().

Passwords are case sensitive.

Password retry

If a user fails to provide the correct password after a number of consecutive retries, the switch resets the logon process.

You can configure the maximum number of retries using the Console Interface (TELNET/SNMP/Web Access, Login Retries field) or ACLI. The default maximum number of retries is 3.

Password history

The switch stores a maximum of the last 10 passwords used. If you set the password for the fourth time and the history size is set to 3, you can reuse the password that you used the first time. You cannot reuse a password stored in history.

Password display

When you type a password, the characters you type are not displayed as clear text. Each character of the password is substituted with an asterisk (*).

Password verification

New passwords must be verified before use. If the two passwords do not match, the password update process fails. In this case, the password change process starts over. Password change attempts have no limit.

Password aging time

Passwords expire after a specified aging period. The aging period is configurable and the range is from 1 to 365 days. The default is 90 days. When a password has aged out, the user is prompted to create a new password. Only users with a valid read-write password can create a new password.

Logon failure timeout

Log on failure timeouts prevent brute force hacking. Following three consecutive password log on failures, all password logon interfaces are disabled for 60 seconds. Logon failure timeouts disable the serial port, Telnet, and Web interfaces.

Log on failure timeouts affect only new log on sessions and do not interfere with sessions already in progress.

Default passwords

For the non-SSH image, the default password for the read–only user is ***user***, and the default password for the read–write user is ***secure***. If your switch supports the SSH software image, the default password for the read–only user is ***userpasswd***, and the default password for the read–write user is ***securepasswd***.

Password security enabled or disabled

By default, password security is disabled for the non-SSH software image. If your switch supports the SSH software image, password security is enabled.

You can enable password security using ACLI only. When password security is enabled, the following occurs:

- Current passwords remain unchanged if they meet the required specifications. If they do not meet the required specifications, the user is prompted to change them to passwords that do meet the requirements.
- An empty password history bank is established. The password bank stores has the capacity to store up to 10 previously used passwords.

- Password verification is required.

You can disable password security using ACLI only. When password security is disabled, the following occurs:

- Current passwords remain valid.
- Password history bank is removed.
- Password verification is not required.

Lockout for failed logon attempts

When a user exceeds the predetermined maximum number of logon retry attempts, the switch denies that user access to all password logon interfaces, such as Telnet, SSH and WEB for a configurable time interval. The default lockout interval is one minute.

The lockout for failed logon attempts feature prevents brute force hacking.

Multiple local RW and RO user accounts

With multiple local read-write (RW) and read-only (RO) user accounts, VSP 7000 Series switches support up to 8 RW and 8 RO user accounts, in addition to the 2 default users. Using multiple user accounts avoids account sharing and helps improve security by making user actions visible through the analysis of audit records.

You can assign new users RW or RO permissions. Each user can access the switch using the local serial port, Telnet, HTTP (WEB), or SSH. Users require a username and password to connect to the switch and authenticating against an external RADIUS or TACACS+ server is supported. RADIUS fallback extends the search for local users, if the RADIUS server is unavailable.

Note:

Each user must have a unique username.

Log files display user RO and RW login information, including the source IP address of the device the user logged in from.

The default RW user can create, remove, or modify other users, except the default RO user, which cannot be deleted.

The audit log displays information containing the username for the authenticated user. Syslog messages display information about when a user logs in or logs out.

If a login attempt fails, the error feedback does not indicate if the failed login is due to an invalid username or an invalid password. Also, response times for an invalid username, and an invalid username and password pair are identical, to prevent identification of which authentication type failed. The passwords are encrypted and do not appear in any log.

Limitations

The following limitations apply:

- The switch supports a maximum of 18 user sessions at one time.
- A new user can log in to a maximum of 10 sessions at one time.
- EDM allows the authentication of any of the 10 supported users, but not more than the number of maximum HTTP or HTTPS sessions.
- Because rebooting a switch or stack to factory default erases all created users, only the administrative user can execute the `boot default` command.
- When you disable Telnet, all users connected to the switch using Telnet are disconnected.
- When you disable SSH, all users connected using SSH are disconnected.
- When a switch unit joins a stack, all users created on the base unit are also created on non-base units.
- After upgrading from a non-SSH build to a SSH build, you must reboot the switch to return all passwords to default.

For more information about configuring multiple local RW and RO user accounts, see

- Configuring Multiple local RW and RO user accounts on page 56
- Displaying local user information on page 64

Simple Network Management Protocol

The Avaya Virtual Services Platform 7000 Series supports Simple Network Management Protocol (SNMP).

SNMP is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device running software that supports the retrieval of SNMP information can be monitored.

You can also use SNMP to change the state of SNMP-based devices. For example, you can use SNMP to shut down an interface on your switch.

SNMP versions

The SNMP agent for the Avaya Virtual Services Platform 7000 Series supports exchanges using SNMPv1, SNMPv2c, and SNMPv3. The following sections provide descriptions for each of these SNMP versions.

SNMP Version 1 (SNMPv1)

SNMP Version 1 (SNMPv1) is an older version of the SNMP protocol that is defined in RFC 1157 and is an Internet Engineering Task Force (IETF) standard. SNMPv1 security is based on

communities, which are simply plain text password strings that allow an SNMP-based application, that knows these strings, to gain access to the management information for a device.

SNMPv1 uses a proprietary method for configuring SNMP communities and trap destinations for specifying SNMPv1 configuration. This proprietary method includes the following:

- A single read-only community string that can only be configured using the console menus.
- A single read-write community string that can only be configured using the console menus.
- Up to four trap destinations and associated community strings that can be configured either in the console menus, or using SNMP Set requests on the s5AgTrpRcvrTable.

SNMP Version 2 (SNMPv2)

SNMP Version 2 (SNMPv2) is also an older version of the SNMP protocol, which is called SNMPv2c, as defined in RFC 1905, RFC 1906, and RFC 1907. SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMP Version 3 (SNMPv3)

SNMP Version 3 (SNMPv3) is the current formal SNMP standard, defined in RFCs 3410 through 3419, and in RFC 3584. SNMPv3 uses a standards-based method of configuring SNMP communities, users, groups, views, and trap destinations. SNMPv3 support applies industrial-grade user authentication and message security, which includes MD5 and SHA-based user authentication, and message integrity verification. SNMPv3 also applies AES, DES, and 3DES based privacy encryption. Export restrictions on SHA and DES necessitate support for domestic and non-domestic executable images or defaulting to no encryption for all customers.

All the configuration data configured using SNMPv1 is mapped into the SNMPv3 tables as read-only table entries. With the SNMPv3 method of configuring SNMP, all processes are configured and controlled through the SNMPv3 MIBs. Avaya Command Line Interface (ACLI) commands can change or display the single read-only community, read-write community, or four trap destinations of the SNMPv1 configuration. Otherwise, the ACLI commands change or display SNMPv3 MIB data.

Important:

You must configure views and users using ACLI before you can use SNMPv3.

Important:

You must have the secure version of the software image installed on your switch before you can configure SNMPv3.

The following table lists the maximum number of nonvolatile entries (entries stored in NVRAM) allowed in SNMPv3 tables. The system does not allow you to create more entries marked nonvolatile when you reach these limits:

SNMPv3 table	Maximum number of NVRAM entries
snmpCommunityTable	20
vacmViewTreeFamilyTable	60
vacmSecurityToGroupTable	40

SNMPv3 table	Maximum number of NVRAM entries
vacmAccessTable	40
usmUserTable	20
snmpNotifyTable	20
snmpTargetAddrTable	20
snmpTargetParamsTable	20

SNMP MIB support

The Avaya Virtual Services Platform 7000 Series supports an SNMP agent with industry-standard Management Information Bases (MIB) as well as private MIB extensions, which ensures compatibility with existing network management tools.

Supported MIBs

The IETF standard MIBS supported on the switch include MIB-II (originally published as RFC 1213, and then split into separate MIBs as described in RFCs 4293, 4022, and 4113), Bridge MIB (RFC 4188), and the RMON MIB (RFC 2819), which provides access to detailed management statistics.

The following table lists supported SNMP standard MIBs.

MIB	RFC	File name
IF-MIB	2863	rfc2863.mib
SNMPv2-MIB	3418	rfc3418.mib
EtherLike-MIB	2665	rfc2665.mib
ENTITY-MIB	2737	rfc2737.mib
P-BRIDGE-MIB	4363	rfc4363-p.mib
Q-BRIDGE-MIB	4363	rfc4363-q.mib
IEEE8021-PAE-MIB	n/a	eapol-d10.mib
SMIv2-MIB	2578	rfc2578.mib
SMIv2-TC-MIB	2579	rfc2579.mib
SNMPv2-MIB	3418	rfc3418.mib
SNMP-FRAMEWORK-MIB	3411	rfc3411.mib
SNMP-MPD-MIB	3412	rfc3412.mib
SNMP-NOTIFICATION-MIB	3413	rfc3413-notif.mib
SNMP-TARGET-MIB	3413	rfc3413-tgt.mib
SNMP-USER-BASED-MIB	3414	rfc3414.mib
SNMP-VIEW-BASED-ACM-MIB	3415	rfc3415.mib
SNMP-COMMUNITY-MIB	3584	rfc3584.mib

The following table lists supported SNMP proprietary MIBs.

MIB	File name
S5-AGENT-MIB	s5age.mib
S5-CHASSIS.MIB	s5cha.mib
S5-CHASSIS-TRAP.MIB	s5ctr.trp
S5-ETHERNET-TRAP.MIB	s5etr.trp
RAPID-CITY-MIB	rapidCity.mib
S5-SWITCH--MIB	s5sbs.mib
BN-IF-EXTENSIONS-MIB	s5ifx.mib
BN-LOG-MESSAGE-MIB	bnlog.mib
S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
BAY-STACK-NOTIFICATIONS-MIB	bsn.mib

SNMP trap support

With SNMP management, you can configure SNMP traps (on individual ports) to be generated automatically for conditions such as unauthorized access attempts or changes in port operating status. You can use ACLI to specify a custom SNMP trap port when a new host receiver is added. The SNMP trap port is stored in NVRAM so that the trap port is saved across switch and stack reboots. The SNMP trap port value is shared among all the units in the stack.

You can configure traps using the SNMPv1 or SNMPv2c or SNMPv3 format. If you do not identify the SNMP version, the system formats the traps in the SNMPv1 format. A community string can be entered if the system requires one.

The switch supports both industry-standard SNMP traps, as well as private Avaya enterprise traps.

You can enable or disable SNMP traps for the following features:

- Rapid Spanning Tree Protocol (RSTP)
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)
- Unicast Storm Control
- Split Multi-Link Trunk (SMLT)
- Open Shortest Path First (OSPF)
- SLPP
- SLPP-guard
- MAC Security
- Intermediate System to Intermediate System (IS-IS)

- Virtual Router Redundancy Protocol (VRRP)
- Authentication, Authorization and Accounting (AAA)

The following table lists SNMP traps that are supported globally and on a per interface basis.

Trap name	Configurable	Sent when
RFC 2863 (industry standard):		
linkUp	For each port	A port link state changes to up.
linkDown	For each port	A port link state changes to down.
RFC 3418 (industry standard):		
authenticationFailure	Global	An SNMP authentication failure.
coldStart	Global	An SNMP entity that supports a notification originator application, is reinitializing itself with a configuration that may have been altered.
warmStart	Global	An SNMP entity that supports a notification originator application, is reinitializing itself with an altered configuration.
s5CtrMIB (Avaya proprietary traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrNewUnitUp	Global	A new component or sub-component is detected.
s5CtrNewUnitDown	Global	A component or sub-component is no longer detected.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrNewHotSwap	Global	A component or sub-component was inserted into or removed from the chassis.
s5CtrNewProblem	Global	A component or sub-component has a warning, nonfatal, or fatal problem condition.
s5CtrProblem	Always on	• Base unit fails. • AC power fails or is restored. • RPSU (DC) power fails or is restored. • Fan fails or is restored.

Trap name	Configurable	Sent when
s5CtrFanDirectionError	Global	A fan component's direction is incorrect.
s5CtrHighTemperatureError	Global	The system is overheated.
s5EtrSbsNewSbsMacAccessViolation	Always on for each port	A MAC address security violation is detected.
s5EtrNewSbsMacAccessViolation	For each port	The switch detects a MAC address-based security violation on a port
s5EtrMacAddressTablesThresholdReached	Global	The MAC address table threshold is reached.
s5EtrSbsMacRemoved	For each port	A MAC address was moved from the MAC security address table.
s5EtrSbsMacTableCleared	Global	The MAC security address table was cleared for all ports.
s5EtrSbsMacTableClearedForPort	For each port	The MAC security address table was cleared for a specific port.
s5EtrSbsMacTableFull	Global	The MAC security address table is full.
entConfigChange	Global	Any hardware change—unit added or removed from stack, GBIC inserted or removed.
risingAlarm	Global	Generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps
fallingAlarm	Global	Generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps
bsnConfigurationSavedToNvram	Global	The switch saved the system configuration to NVRAM.
bsnStackManagerReconfiguration	System-wide	The stack manager in a stackable system detects a problem with a link between stack members.
bsnStackConfigurationError	Global	The expected size of a stack is not equal to the actual size of the stack.
bsnEnteredForcedStackMode	Global	A switch has entered the forced stack mode.
bsnSystemUp365Days	Global	The system has been up for 365 days.
bsnTrunkPortDisabledToPreventBroadcastStorm	For each port	An MLT port is disabled because an MLT trunk is disabled.
bsnTrunkPortEnabledToPreventBroadcastStorm	For each port	An MLT port is enabled because an MLT trunk is enabled.

Trap name	Configurable	Sent when
bsnLacPortDisabledDueToLossOfVLACPDU	For each port	A port is disabled due to the loss of a VLACP PDU.
bsnLacPortEnabledDueToReceiptOfVLACPDU	For each port	A port is enabled after receiving a VLACP PDU.
bsnLoginFailure	Global	An attempt to login to the system failed as a result of an incorrect password.
bsnUSBInsertion	Global	A USB device has been inserted.
bsnUSBRemoval	Global	A USB device has been removed.
bsnSFPInsertion	For each port	A SFP module has been inserted.
bsnSFPRemoval	For each port	A SFP module has been removed.
bsnROPasswordExpired	Global	The Read Only password has expired.
bsnRWPasswordExpired	Global	The Read Write password has expired.
ntnQosPolicyEvolLocalUbpSessionFailure		
ntnQosPolicyEvolDosAttackDetected		
rcnSlppPortDownEventNew	Global	A port down event that has occurred due to SLPP.
rcnSlppGuardHoldDownExpired	For each port	Indicates that the SLPP-guard hold-down timer has expired on a port on which SLPP-guard is enabled, and the port has been re-enabled.
rcnSlppGuardPacketReceived	For each port	Indicates an SLPP packet has been received on a port on which SLPP-guard is enabled. The port has been disabled.
rcnBpduReceived	For each port	A BPDU is received on a port that has BPDU filtering enabled.
avFcoeRedirEgressIssueDetected	Global	A FCoE redirect egress issue occurred.
slaMonitorAgentExceptionDetected	Global	A SLA Mon™ agent exception occurred.
RAPID-SPANNING-TREE-MIB:		
nnRstGeneralEvent	Global	Any general event, such as protocol up or protocol down, occurs.
nnRstErrorEvent	Global	Any error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.

Trap name	Configurable	Sent when
nnRstNewRoot	Global	A new root bridge is selected in the topology.
nnRstTopologyChange	Global	A topology change is detected.
nnRstProtocolMigration	Global	A port protocol migration occurred.
nnRstGenNotificationType	System-wide	Any of the general events like protocol up or protocol down occur.
nnRstErrNotificationType	System-wide	Any of the error events like memory failure, buffer failure, protocol migration, new root topology or topology change occur.
nnRstDot1wOldDesignatedRoot	System-wide	A new root bridge is selected in the topology.
nnRstPortNotificationMigrationType	System-wide	A port migration happens in the port.
DHCP Snooping		
bsDhcpSnoopingBindingTableFull	Global	An attempt is made to add a new DHCP binding entry when the binding table is full.
bsDhcpSnoopingTrap	For each port	A DHCP packet is dropped.
bsDhcpOption82MaxLengthExceeded	Global	The DHCP Option 82 information could not be added to a DHCP packet because the resulting packet would be too long.
bsDhcpSnoopingExtSave	System-wide	
bsDhcpSnoopingExtSaveEntryMACConflict	Global	A DHCP snooping binding entry is not restored from an external file due to a MAC conflict.
bsDhcpSnoopingExtSaveEntryInvalidInterface	Global	A DHCP snooping binding entry is not restored from an external file due to an non-existing interface.
bsDhcpSnoopingExtSaveEntryLeaseExpired	Global	A DHCP snooping binding entry is not restored from an external file because the client lease expired.
bsDhcpSnoopingExtSaveEntryParsingFailure	Global	A DHCP snooping binding entry is not restored from an external file due to a parsing failure.
bsDhcpSnoopingExtSaveNTP	Global	The DHCP snooping external save feature is enabled without synchronizing the switch to a NTP server.
bsDhcpSnoopingExtSaveUSBSyncSuccess	Global	The DHCP snooping binding table is successfully saved to a USB drive external file.

Trap name	Configurable	Sent when
bsDhcpSnoopingExtSaveTFTPSyncSuccess	Global	The DHCP snooping binding table is successfully to a TFTP server external file.
bsDhcpSnoopingExtSaveUSBSyncFailure	Global	The DHCP snooping binding table is not successfully saved to a USB drive external file.
bsDhcpSnoopingExtSaveTFTPSyncFailure	Global	The DHCP snooping binding table is not successfully saved to a TFTP server external file.
bsDhcpSnoopingExtSaveUSBRestoreSuccess	Global	The DHCP snooping binding table is successfully restored from a USB drive external file.
bsDhcpSnoopingExtSaveTFTPRestoreSuccess	Global	The DHCP snooping binding table is successfully restored from a TFTP server external file.
bsDhcpSnoopingExtSaveUSBRestoreFailure	Global	The DHCP snooping binding table is not successfully restored from a USB drive external file.
bsDhcpSnoopingExtSaveTFTPRestoreFailure	Global	The DHCP snooping binding table is not successfully restored from a TFTP server external file.
bsDhcpSnoopingExtSaveEntryInvalidVlan	Global	A DHCP snooping binding entry is not restored from an external file due to invalid Vlan ID.
DAI		
bsaiArpPacketDroppedOnUntrustedPort	For each port	An ARP packet is dropped on an untrusted port due to invalid IP/MAC binding.
IP Source Guard		
bsSourceGuardReachedMaxIpEntries	For each port	The maximum IP entries on the port has been reached.
bsSourceGuardCannotEnablePort	For each port	Insufficient resources are available to enable IPSG on the port.
UnicastStormControl		
bsUnicastStormControlBelowLowWatermark	Global	The unicast storm control packet rate falls below the low watermark after having risen above the high watermark.
bsUnicastStormControlAboveHighWatermark	Global	Generated periodically when the unicast storm control packet rate remains above the high watermark.
SMLT		
rcnSmltIstLinkUp	Global	The IST transitions from down to up.

Trap name	Configurable	Sent when
rcnSmltIstLinkDown	Global	The IST transitions from up to down..
rcnSmltLinkUp	Global	SMLT current type transitions from NORM to SMLT. SMLT on both aggregation DUTs is up.
rcnSmltLinkDown	Global	SMLT current type transitions from SMLT to NORM. SMLT on one or both aggregation DUTs is down or disabled.
LLDP		
lldpRemTablesChange	Global	The value of **lldpStatsRemTableLastChangeTime** is changed.
lldpXMedTopologyChangeDetected	For each port	A notification generated by the local switch sensing a change in the topology that indicates that a new remote device is attached to a local port, or a remote device is disconnected, or moved from one port to another.
VRRP		
vrrpTrapNewMaster	Global	The sending agent has transitioned to the '**Master**' state.
bsveVrrpTrapStateTransition	Global	A state transition occurs on a specific VRRP interface.
OSPF		
ospfVirtIfStateChange	Global	Generated when the interface state regresses (for example, goes from Point-to-Point to Down) or progresses to a terminal state (for example, Point-to-Point)
ospfNbrStateChange	Global	Generated when the neighbor state regresses (for example, goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (for example, 2-Way or Full).
ospfVirtNbrStateChange	Global	Generated when the virtual neighbor state regresses (for example, goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (for example, Full).
ospfIfConfigError	Global	A packet has been received on a non-virtual interface from a router for which configuration parameters

Trap name	Configurable	Sent when
		conflict with the configuration parameters of the local router.
ospfVirtIfConfigError	Global	A packet is received on a virtual interface from a router for which configuration parameters conflict with the configuration parameters of the local router.
ospfIfAuthFailure	Global	A packet is received on a non-virtual interface from a router for which the authentication key or authentication type conflicts with the authentication key or authentication type of the local router.
ospfVirtIfAuthFailure	Global	A packet is received on a virtual interface from a router for which the authentication key or authentication type conflicts with the authentication key or authentication type of the local router.
ospfIfStateChange	Global	A change occurs in the state of a non-virtual OSPF interface. This trap is generated when the interface state regresses (for example, goes from Dr to Down) or progresses to a terminal state (for example, Point-to-Point, DR Other, Dr, or Backup).
IS-IS		
rcnIsisPlsbMetricMismatchTrap	Global	An LSP with a different value of L1-metric is received.
rcnIsisPlsbDuplicateSysidTrap	Global	A Hello packet with a duplicate system ID is received.
rcnIsisPlsbLsdbUpdateTrap	Global	LSDB information is changed.
rcnIsisPlsbBvidMismatchTrap	Global	A Hello packet with mismatched LSDB-VIDs is received
rcnIsisPlsbAdjStateTrap	Global	The ISIS adjacency state change.
rcnIsisPlsbDuplicateNnameTrap	Global	An LSP with duplicate a nickname is received.
rcnIsisPlsbMultiLinkAdjTrap	Global	Multiple ISIS adjacencies are formed with the same ISIS node.
LACP		
bsnLacTrunkUnavailable	Global	An attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk.

Trap name	Configurable	Sent when
AAA		
bsnAaaUserAccountNotUsed	Global	If a user account is never used during a time interval.
bsnAaaAlreadyConnected	Global	Attempt to connect when already connected.
bsnAaaIncorrectLogOnThresholdExceeded	Global	Threshold for entering the incorrect information exceeds.
bsnAaaMaxNoOfSessionsExceeded	Global	Maximum number of current sessions for an AAA user account exceeds.

SNMP trap control per port notification

With the "SNMP notification-control" feature, traps are defined on a global basis (per bridge) such as bsnConfigurationSavedToNvram. You can enable or disable notifications globally, and for some traps on a per interface basis.

With SNMP trap control, the supported notifications such as linkDown, linkup can be enabled or disabled on per interface basis, as well as globally.

Note:

All notifications are enabled on individual interfaces by default.

When a notification per interface is disabled, notification events will not be sent.

The following SNMP Traps are supported per interface:

- linkDown
- linkUp
- lldpXMedTopologyChangeDetected
- bsDhcpSnoopingTrap
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort
- rcnBpduReceived
- bsnTrunkPortDisabledToPreventBroadcastStorm
- bsnTrunkPortEnabledToPreventBroadcastStorm
- bsnLacPortDisabledDueToLossOfVLACPDU
- bsnLacPortEnabledDueToReceiptOfVLACPDU
- bsnSFPInsertion
- bsnSFPRemoval
- s5EtrSbsMacTableClearedForPort

- s5EtrSbsMacRemoved
- s5EtrNewSbsMacAccessViolation

SNMP interaction with other features

This section provides information about how SNMP interacts with other switch features.

If your switch supports Dynamic Host Control Protocol (DHCP) and DHCP is disabled globally, SNMP traps for DHCP Snooping cannot be generated.

Secure Shell protocol

The Secure Shell (SSH) protocol provides secure remote login and other secure network services over an insecure network and replaces Telnet for sustaining secure access to the Avaya Command Line (ACLI) interface.

The SSH protocol recognizes two major versions; SSH1 and SSH2. SSH implementation for the Avaya Virtual Services Platform 7000 Series supports the SSH2 version.

SSH2 components

SSH2 is comprised of the following three major components:

- The SSH Transport Layer Protocol (SSH-TRANS) is one of the fundamental SSH2 building blocks. SSH-TRANS provides initial connection, packet protocol, server authentication, basic encryption, integrity services, and can also provide compression. The transport layer is used over a TCP/IP connection and can be used on top of other reliable data streams.
- The SSH User Authentication Protocol (SSH-USERAUTH) authenticates the client-side user to the server and functions with the transport layer protocol. SSH-AUTH supports two methods: public key and password authentication. To authenticate, an SSH2 client tries a sequence of authentication methods chosen from the set allowed by the server (for example, public key and password) until one succeeds or all fail.
- The SSH Connection Protocol (SSH-CONNECT) multiplexes the encrypted tunnel into several logical channels. SSH-CONNECT functions with the user authentication protocol.

SSH service configuration

With the SSH service engine, you can configure the SSH service on the switch using the ACLI, EDM, or SNMP interfaces.

Important:

If you enable SSH on the switch and you load an ASCII configuration file containing SSH related commands, those commands will fail. You must disable SSH on the switch before you load an ASCII configuration file containing SSH related commands.

SSH service management objects are:

- SSH enable or disable

  The switch operates in SSH secure mode when you enable SSH and configure the SSH server to disable non-secured interfaces. When you enable SSH but you do not configure the SSH server to disable non-secured interfaces, the switch operates in unsecured SSH mode.

- DSA authentication enable or disable

  You can configure the SSH server to allow or disallow DSA authentication.

- RSA authentication enable or disable

  You can configure the SSH server to allow or disallow RSA authentication.

- Password authentication enable or disable

  If you do not enable password authentication you cannot initiate connections using password authentication, but you can initiate connections using publickey (DSA or RSA) authentication. After you have access, you cannot disable both DSA and password authentication.

  The SSH authentication retries parameter of the SSH server refers to all available SSH authentication types (Password authentication, DSA public key authentication, and RSA public key authentication). The default SSH authentication retries is three.

- DSA public key upload and download
- RSA public key upload and download
- SSH information dump: shows all the SSH-related information

Supported SSH clients

The switch supports the following SSH clients:

- Putty SSH (Windows 2000)
- F-secure SSH, v5.3 (Windows 2000)
- SSH Secure Shell 3.2.9 (Windows 2000)
- SecureCRT 4.1
- Cygwin OpenSSH (Windows 2000)
- AxeSSH (Windows 2000)
- SSHPro (Windows 2000)

- Solaris SSH (Solaris)
- Mac OS X OpenSSH (Mac OS X)

SSH and SSH Client

Secure Shell (SSH), a network protocol, uses a secure channel to exchange data between two network devices. Remote login to execute commands is a typical use of SSH. SSH also supports file transfer (using SFTP or SCP protocols), tunneling, forwarding TCP ports and X11 connections. SSH uses the client-server model to provide confidentiality and integrity of data over an unsecured / public network, such as the Internet.

SSH Client is a secure shell protocol for connecting to an SSH Server device in the network that is accepting remote connections. SSH Client is supported only on switches running the SSH image and can be configured only with the ACLI interface.

The Avaya-implemented SSH Client uses SSH version 2 protocol (SSH-2) to provide an SSH Client session.

SSH Client can use DSA or RSA authentication keys. If key authentication fails due to non-existent or unaccepted DSA or RSA keys, you can enter a username and password, for which the system supports a maximum of three tries. To end the SSH session and return to ACLI, enter a '~' followed by a period (~.). The SSH Client session blocks the ACLI or Console session, so the SSH loop runs on Console task. To break the SSH loop at any time, you can use the '~.' character pair. The SSH loop does not include the connection initialization part. If the Console session closes, the inner SSH Client also terminates.

Note:

You can open only one SSH Client session. The switch does not support multiple SSH Client sessions.

SSH Client known hosts

To support the key method of authentication, the switch saves a list of SSH Client known host information (such as, host IP address and public key signature entries) in NVRAM. The switch identifies a host as known when it recognizes the signature of the host public key. Administrators and users with read-only or read-write access have access to known hosts.

When SSH connects to a host and receives the host public key, the switch calculates the signature of the received key. The switch accepts the host if the host IP address and received public key signature pair matches the host IP address and public key signature in the known host list. If key signatures do not match, the SSH Client ends the connection.

If the host IP address does not match an entry in the known host list, you can accept or decline the host IP address and received public key association. If you accept the host, the switch updates the known host list and the switch accepts the connection.

If you have read-write access, you can delete hosts, by host IP address, from the known host list, using ACLI.

Because the switch only consults the known host list during SSH connection, you do not affect an existing connection if you delete or modify known host information during an active SSH session.

After you reset the switch to default, the switch empties the SSH known-hosts list.

SSH Client known hosts in a stack environment

During stack formation, the base unit synchronizes the known host lists on all stack units and removes deleted known hosts from the lists. SSH Client initialization updates the known host lists on all units in the stack with information from the known host list on the base unit.

To maintain secure access integrity for switch stacks, the system saves any known host list information updates in the NVRAM of all switches in the stack. If the base unit is removed from the stack, or a break in the stack occurs, the remaining stack units retain the learned host information.

Authentication key storage capacity

Each switch can store DSA and RSA authentication keys for a minimum of 20 SSH Client known hosts.

SSH Client feature interactions

SSH Client interacts and shares DSA and RSA keys, and key sizes with SFTP Client.

Secure Socket Layer protocol

Secure Socket Layer (SSL) provides a secure Web management interface.

The SSL server includes the following features:

- SSLv3-compliant
- Supports PKI key exchange
- Uses key size of 1024-bit encryption
- Supports RC4 and 3DES cryptography
- Supports MAC algorithms MD5 and SHA-1

An SSL certificate is generated when:

- the system is powered up for the first time and the NVRAM does not contain a certificate that can be used to initialize the SSL server.
- the management interface (ACLI/SNMP) requests that a new certificate to be generated. A certificate cannot be used until the next system reset or SSL server reset.

Web server secure and non-secure modes

The Web server can operate in either HTTPS (secure) mode or HTTP (non-secure) mode, with HTTPS as the default mode. You can select the Web server mode with the ACLI and SNMP management interfaces. The SSL Management Library interacts with the Web server in selecting these modes.

In secure mode, you can use the **`https-only`** command to configure the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

By default, the Web server listens on TCP port 443 for HTTPS client browser requests, and listens on TCP port 80 for HTTP client browser requests. You can designate alternate TCP ports, ranging in value from 1024 to 65535, for HTTPS and HTTP client browser requests.

Important:

The TCP port for HTTPS client browser requests and the TCP port for HTTP client browser requests cannot be the same value.

In non-secure mode, the Web server responds to HTTP client browser requests only. All existing secure connections with the browser are terminated.

SSL Certificate Authority

Generally, an SSL certificate is issued and signed by a Certificate Authority (CA), such as VeriSign. Because the management and cost of purchasing a certificate from the CA is a concern, Avaya issues and signs the SSL certificate, with the understanding that Avaya is not a recognized Certificate Authority. Ensure that client browsers that connect to the Avaya Virtual Services Platform 7000 Series, SSL-enabled Web management interface are aware of this fact.

The SSL certificate contains the information shown as follows. The first three lines are constant. The rest is derived from the RSA host key associated with the certificate.

```
Issuer     : Avaya
Start Date : May 26 2003, 00:01:26
End   Date : May 24 2033, 23:01:26

RSA Host Key (length= 1024 bits):
94111167c35082b3d050a2964a4e573e6918162ce57c525adde001cc67abfa83
ac293823412affd02e21ad51061a7466000ad6b9307d80a3f33309444b58e7f5
68985559fc7433e7296ba7e108bb2aa152dd682f6133c922ad245310cbe70d60
00868887a8445ac702d65f9ceb7a3e6c1481664425c11dc67bbb2fe9999abecd
```

Secure File Transfer Protocol

For switches running a secure software image, with Secure Shell (SSH) enabled, you can enhance network security by using Secure File Transfer Protocol (SFTP) to transfer files between a switch or stack and an SFTP server that supports SSH version 2 (SSHv2).

With SFTP over SSH, you can perform the following file transfers with a higher level of security than basic SFTP:

- uploading binary configuration files to an SFTP server
- downloading binary configuration files from an SFTP server
- uploading ASCII configuration files to an SFTP server
- downloading ASCII configuration files from an SFTP server
- DSA key authentication support
- RSA key authentication support
- password authentication
- host key generation
- 512–1024-bit DSA-key use for authentication
- 1024–2048-bit RSA-key use for authentication

SFTP is enabled by default and interacts with SSH client.

RADIUS–based network security

The Remote Authentication Dial-In User Service (RADIUS) protocol provides centralized authentication, authorization, and accounting for network access. RADIUS is a distributed client and server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate user identities through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges, protected with a shared secret.

RADIUS authentication is a fully open and standard protocol defined by RFC 2865.

The RADIUS application includes the following two components:

- RADIUS server—a computer equipped with server software (for example, a UNIX workstation) located at a central office or campus. It has authentication and access information in a form compatible with the client.
- RADIUS client—a switch, router, or remote access server equipped with client software that typically resides on the same network segment as the server. The client is the network access point between the remote users and the server.

With RADIUS authentication, a remote server can authenticate users that attempt to log on to the switch from a local console or Telnet session.

Avaya recommends that you include two RADIUS servers in a Virtual Services Platform 7000 Series network: a primary RADIUS server and a secondary RADIUS server for backup. The secondary server is used only if the primary server is unavailable or unreachable. You identify the primary and secondary server when you configure the RADIUS servers on the switch.

RADIUS permits a configuration of one to five retries, with a default of three retries for service requests to each RADIUS server in the network. You can configure the timeout interval between each retry.

RADIUS server configuration

You must configure specific user accounts on the RADIUS server before you can use RADIUS authentication in the Virtual Services Platform 7000 Series network. User account information about the RADIUS server includes user names, passwords, and Service-Type attributes.

Provide each user with the appropriate level of access.

- for read-write access, set the Service-Type field value to *Administrative*.
- for read-only access, set the Service-Type field value to *NAS-Prompt*.

For detailed information about configuring the RADIUS server, see the documentation that came with the server software.

Change RADIUS password

You can allow remote users to change their account passwords when you have RADIUS configured and enabled in your network.

Note:

Change RADIUS password is available only in secure software builds.

After you configure RADIUS servers in your network to provide centralized authentication, authorization and accounting for network access, you can enable the MS-CHAPv2 encapsulation method, which permits the changing of the RADIUS password for user accounts.

Change RADIUS password is disabled by default.

If you enable RADIUS encapsulation ms-chap-v2, when an account password expires the RADIUS server reports the expiry during the next log on attempt, and the system prompts you to create a new password. You can also change the password before the password expires using ACLI.

To use change RADIUS password you must have:

- at least one configured and reachable RADIUS server in your network
- configured RADIUS encapsulation ms-chap-v2

Change RADIUS password is compatible with RADIUS password fallback.

Settings for the change RADIUS password feature are saved in both the binary and ASCII configuration files.

Effects of software upgrade on RADIUS settings:

The system saves all RADIUS settings in NVRAM so, if you upgrade the switch software, the new image loads the settings.

Effects of software downgrade on RADIUS settings:

Once you downgrade the switch software, the change RADIUS password configuration defaults if it is available on the release.

RADIUS password fallback

The RADIUS password fallback feature lets the user log on to the switch or stack by using the local password if the RADIUS server is unavailable or unreachable for authentication.

RADIUS password fallback is disabled by default.

RADIUS management accounting

You can use the RADIUS Management Accounting feature to send RADIUS accounting packets when management events such as user logon, user logoff, or session timeout occur. RADIUS management accounting can record management logon activity to the switch. The switch generates and sends an accounting packet to the RADIUS server, which includes basic information such as NAS-IP-Address, Service-Type, User-Name, Client-IP-Address, and Timestamp.

RADIUS management accounting records are generated when the switch is accessed using the console, Telnet, SSH, or when a session is disconnected either by logging out or through time-out.

The following table describes the additional information fields in the RADIUS accounting message. This information enhances the interoperability of the switch in environments where other vendors use their switches.

Table 3: RADIUS Management Accounting Records

RADIUS attribute	Definition
NAS-IP-Address	The IP address of the device generating the RADIUS accounting message (the switch or stack IP address).
NAS-IPv6-Address	The IPv6 address of the device generating the RADIUS Accounting message (the switch or stack address).
NAS-Port-Type	The type of port through which the connection is made to the switch, as defined in RFC2865. For a logon through the console port, the port type corresponds to **Async** or **Virtual** for the network connections.

RADIUS attribute	Definition
NAS-Port	Equal to the unit number in a stack if the customer uses the console port. If the connection is **Virtual**, this value is 0.
Service-Type	Set to *Administrative-User* for access to the switch or stack with read-write rights. Set to *NAS-Prompt-User* for access to the switch or stack with read-only rights.
User-Name	The user name used to connect the current administrative session to the switch.
Acct-Status-Type	Indicates if this is an accounting Start or Stop record, used to respectively identify connection or disconnection to or from the switch.
Acct-Terminate-Cause	Used in the accounting stop records that the switch generates after a session is disconnected from the switch. Possible values includes the following options. • User-Request—used when user signs off. • Idle-Timeout—used when timeout occurs. • Lost-Carrier—used when a serial login was performed and the serial cable is unplugged (works with serial security enabled).
Client-IP-Address	The end client IP address, if the customer connects through IP. If the customer connects through the console, the end client IP address is the same as the switch or stack IP address.
Timestamp	The timestamp of the RADIUS accounting record.

RADIUS use management IP

When the switch is operating in Layer 3 mode, by default, a RADIUS request uses one of the routing IP addresses on the switch. In Layer 3 mode, the RADIUS use management IP configuration ensures that the switch or stack generates RADIUS requests using the source IP address of the in-band management VLAN. In some networks, the source IP in the RADIUS request is used to track management access to the switch.

When the switch is operating in Layer 2 mode, by default, all RADIUS requests generated by the switch use the stack or switch in-band management IP address as the source address in RADIUS requests or status reports. The RADIUS use management IP configuration has no impact when the switch operates in Layer 2 mode.

Note:

If the management VLAN is not operational, the switch cannot send any RADIUS requests when:

- the switch is operating in Layer 2 mode.

- the switch is operating in Layer 3 (routing) and RADIUS use management IP is enabled.

This is normal behavior. In Layer 2 mode, if the management VLAN is unavailable, there is no active management IP instance. In Layer 3 mode, if RADIUS use management IP is enabled, then the switch does not use any of the other routing instances to send RADIUS requests when the management VLAN is inactive or disabled.

Applications and MIB filenames

The following table shows supported applications, related MIBs, and the MIB filenames.

Table 4: Application and related MIBs

Application	Related MIBs	File name
Autotopology	S5-ETH-MULTISEGTOPOLOGY-MIB	s5emt.mib
	S5-SWITCH--MIB	s5sbs.mib
MIB-2	RFC1213-MIB	rfc1213.mib
MultiLink Trunking (MLT)	RAPID-CITY-MIB (rcMlt group)	rcMlt.mib
RMON-MIB	RMON-MIB	rfc2819.mib
Spanning Tree	BRIDGE-MIB	rfc4188.mib
System log	BN-LOG-MESSAGE-MIB	bnlog.mib
VLAN	RAPID-CITY-MIB (rcVlan group)	rcVlan.mib

Table 5: New MIBs

MIB name	RFC	File name
BAY-STACK-ERRORMESSAGE- MIB	1271	Rfc1271.mib

TACACS+

The Avaya Virtual Services Platform 7000 Series supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client and server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server (NAS).

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol.
- TACACS+ uses full packet encryption, rather than just encrypting the password (RADIUS authentication request).

Important:

TACACS+ encrypts the entire body of the packet but uses a standard TACACS+ header.

TACACS+ separates authentication, authorization, and accounting services, which means that you can selectively implement one or more TACACS+ services.

TACACS+ provides management of users who access the switch through Telnet, serial, and SSH v2 connections. TACACS+ supports only users connecting to a router or network access server using ACLI.

Access to the Web server interface and SNMP are disabled when TACACS+ is enabled. If you enable the Web server when TACACS+ is enabled, the local database is used for Web server user authentication.

For more information about TACACS+, see http://www.microsoft.com.

TACACS+ terminology

The following terms are commonly used in association with TACACS+:

- AAA—Authentication, Authorization, Accounting
  - Authentication—the action of determining who a user (or entity) is, before allowing the user to access the network and network services.
  - Authorization—the action of determining what an authenticated user is allowed to do.
  - Accounting—the action of recording what a user is doing or has done.
- NAS—a client, such as an Avaya Virtual Services Platform 7000 Series device, that makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets.
- daemon/server—a program that services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
- attribute=value (AV) pairs—strings of text in the form **attribute=value**, sent between a NAS and a TACACS + daemon as part of the TACACS+ protocol.

TACACS+ architecture

You can configure TACACS+ on the Avaya Virtual Services Platform 7000 Series using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port, a serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the Avaya Virtual Services Platform 7000 Series.
- Connect the TACACS+ server through the management interface using an out-of-band management network.

You can configure a secondary TACACS+ server for backup authentication. You must configure the switch for TACACS+ before you can specify the primary and secondary authentication servers.

TACACS+ operation

During the logon process, the TACACS+ client initiates the TACACS+ authentication session with the server. After successful authentication, if TACACS+ authorization is enabled, the TACACS+ client initiates the TACACS+ authorization session with the server. After successful authentication, if TACACS+ accounting is enabled, the TACACS+ client sends accounting information to the TACACS+ server.

TACACS+ authentication

TACACS + authentication offers complete control of authentication through logon and password dialog and response. The authentication session provides username and password functionality.

You cannot enable both RADIUS and TACACS+ authentication on the same interface. However, you can enable RADIUS and TACACS+ on different interfaces; for example, you can enable RADIUS on the serial connection and TACACS+ on the Telnet connection.

Important:

Logon and password prompts appear prior to the authentication process. If TACACS+ fails because there are no valid servers, the username and password are used for the local database. If TACACS+ or the local database return an access denied packet, the authentication process stops, and no other authentication methods are attempted.

TACACS+ authorization

The transition from TACACS+ authentication to the authorization phase is transparent to the user. When the authentication session is successfully completed, an authorization session starts with the authenticated username. The authorization session provides access level functionality.

With TACACS+ authorization, you can limit the switch commands available to a user. When TACACS+ authorization is enabled, the NAS uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user session. The user is granted access to a requested command only if the information in the user profile allows access.

TACACS+ authorization is not mandatory for all privilege levels.

After the NAS requests authorization, the entire command is sent to the TACACS+ daemon for authorization. You preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments, and associating each command with an action to deny or permit.

Authorization is recursive over groups. If you place a user in a group, the daemon looks in the group for authorization parameters if it cannot find them in the user declaration.

If authorization is enabled for a privilege level to which a user is assigned, the TACACS+ server denies commands for which access is not explicitly granted for the specific user or for the user group. On the daemon, ensure that each group is authorized to access basic commands such as **`enable`** or **`logout`**.

If the TACACS+ server is not available or an error occurs during the authorization process, the only command available is **`logout`**.

In the TACACS+ server configuration, if no privilege level is defined for a user but the user is allowed to execute at least one command, the user defaults to privilege level 0. If all commands are explicitly denied for a user, the user cannot access the switch at all. To support runtime switching of users to a particular privilege level, you must preconfigure a dummy user on the TACACS+ server for that level on the daemon. The format of the user name for the dummy user is `$enab<n>$`, where *<n>* specifies the privilege level to which you want to allow access.

TACACS+ accounting

With TACACS+ accounting, you can track the following:

- services accessed by users
- amount of network resources consumed by users

When you enable TACACS+ accounting, the NAS reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting attribute=value (AV) pairs. The accounting records are stored on the security server. The accounting data can be analyzed for network management and auditing.

TACACS+ accounting provides information about user ACLI terminal sessions within serial, Telnet, or SSH shells (from ACLI management interface).

The accounting record includes the following information:

- user name
- date
- start, stop, and elapsed time
- access server IP address
- reason

You cannot customize the set of events that are monitored and logged by TACACS+ accounting.

TACACS+ accounting logs the following events:

- user logon and logoff
- logoff generated because of activity timeout
- unauthorized command
- Telnet session closed (not logged off)

TACACS+ feature limitations

The Avaya Virtual Services Platform 7000 Series does not support the following features with the current TACACS+ implementation:

- S/KEY (One Time Password) authentication.
- PPP/PAP/CHAP/MSCHAP authentication methods.
- The FOLLOW response of a TACACS+ server, in which the AAA services are redirected to another server. The response is interpreted as an authentication failure.
- The user capability to change passwords at runtime over the network. The system administrator must change user passwords locally, on the server.

DHCP snooping

When you use Dynamic Host Configuration Protocol (DHCP) servers in a network to allocate IP addresses to network clients, you can configure DHCP snooping on network switches to allow only clients with specific IP or MAC addresses to access the network.

With DHCP snooping, you can prevent attackers from responding to requests from DHCP servers with false IP or MAC information. DHCP snooping defends against this type of attack, known as DHCP spoofing, by performing as a firewall between untrusted hosts and the DHCP servers.

DHCP snooping classifies switch ports into the following two types:

- Untrusted—ports configured to receive messages from outside the network or firewall. For untrusted ports, only DHCP requests are allowed.

  Trusted—ports configured to receive messages only from within the network, such as switch-to-switch and DHCP server ports. For trusted ports, all types of DHCP messages are allowed.

DHCP snooping can eliminate the man-in-the-middle attack capability to set up rogue DHCP servers on untrusted ports by:

- allowing only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages from untrusted ports are dropped.
- verifying the source of DHCP packets as follows:
  - When the switch receives a DHCP request on an untrusted port, DHCP snooping compares the source MAC address and the DHCP client hardware address. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

    Important:

    This verification is applicable only in Layer 2 mode.
  - When the switch receives a DHCP release or DHCP decline broadcast message from a client, DHCP snooping verifies that the port on which the message was received matches

the port information for the client MAC address in the DHCP binding table. If the port information matches, the switch forwards the DHCP packet.

You must configure DHCP snooping individually for each VLAN. You can configure DHCP snooping using ACLI, EDM, or SNMP

DHCP snooping binding table

When enabled, DHCP snooping dynamically creates and maintains a binding table. The DHCP snooping binding table includes the following information about DHCP leases on untrusted interfaces:

- source MAC address
- IP address
- lease duration
- time until expiration of current entry
- VLAN ID
- port
- source information that can be learned or is static

The maximum size of the DHCP snooping binding table is 1024 entries.

The DHCP snooping binding table is used by IP Source Guard to filter traffic. If the sending station is not in the binding table, no IP traffic is allowed to pass. When a connecting client receives a valid IP address from the DHCP server, IP Source Guard installs a filter on the port to allow only traffic from the assigned IP address.

Static DHCP binding table entries

You can manually add static entries in the DHCP binding table to protect IP devices using applications such as DAI and IPSG, that rely on DHCP snooping table entries. When the protection of these statically configured IP devices is no longer required, you can manually delete entries from the DHCP binding table.

Static DHCP binding table entries with infinite expiry time are stored in NVRAM and are saved across restarts.

DHCP snooping binding table external save

You can use DHCP snooping external save to store the DHCP snooping database at predefined, 5 minute intervals, to an external TFTP server or USB drive.

When the DHCP snooping external save feature is enabled, the switch monitors changes to the DHCP snooping database. If a change is detected, the sync flag is set to true, and when the five minute interval is reached, the binding database saves to the selected TFTP server or USB drive. In

the event of a reboot, the switch attempts to restore the DHCP snooping database with the externally saved file. If the switch learns duplicate DHCP addresses or processes duplicate DHCP requests between the completion of the reboot process and when the DHCP snooping database is restored from the externally saved file, the new information takes precedence over the information from the restored file.

You must enable SNTP/ NTP and synchronization. The lease expiry time the switch writes to the externally saved DHCP snooping database is the absolute lease expiry time, which can be accurately restored from the external save when you reboot the switch.

Important:

Any DHCP snooping database entries that you manually configure, or that the switch learns between the time of the last initiated external save and the beginning of the reboot process are lost and not available when the switch is again operational.

Feature limitations

Be aware of the following limitations:

- Routed, tagged DHCP packets can bypass DHCP snooping filters due to the VLAN changes when a packet is rerouted in Layer 3 mode. This limitation does not apply to Layer 2 VLANs.
- Routed DHCP packets bypass source MAC address and client hardware address verification because this type of verification is not applicable in Layer 3 mode.

Important:

Violating DHCP Release or Decline packets may interrupt communication between the server and the client. Avaya recommends restarting the communication or clearing the ARP cache on the server, after the violating traffic is stopped.

DHCP snooping Option 82

When you enable DHCP snooping Option 82, the switch can transmit information about the DHCP client to the DHCP server. The server can use the information from the switch to locate the DHCP client in the network and allocate a specific IP address to the DHCP client.

DHCP snooping Option 82 function is controlled by the one switch at the edge of a network and not by any switches located between the network edge switch and the DHCP server.

DHCP snooping Option 82 cannot function independently from DHCP snooping (Layer 2 mode).

Dynamic ARP inspection

Dynamic Address Resolution Protocol (ARP) inspection is a security feature that inspects and validates ARP packets in a network.

Without dynamic ARP inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and by intercepting traffic intended for other hosts on the subnet. Dynamic ARP inspection prevents this type of attack by intercepting, logging, and discarding ARP packets with invalid IP-to-MAC address bindings.

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table. For more information about the DHCP binding table, see the **DHCP snooping binding table** section in this guide.

When you enable dynamic ARP inspection, ARP packets on untrusted ports are filtered based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. ARP packets for which the source MAC and IP address do not match an entry in the address binding table are dropped.

The function of dynamic ARP inspection is dependant on DHCP snooping being globally enabled.

Dynamic ARP inspection is configured on a VLAN to VLAN basis.

Feature limitations

Routed, tagged ARP packets can bypass Dynamic ARP Inspection filters due to the VLAN changes when a packet is rerouted in Layer 3 mode. This limitation does not apply to Layer 2 VLANs.

IP Source Guard

IP Source Guard (IPSG) is a Layer 2, port-to-port basis feature that provides security to a network by using information in the DHCP snooping binding table to filter clients with invalid IP addresses. When you enable IPSG on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP binding table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IPSG-enabled port. When this number is reached, no more filters are set up and traffic is dropped.

Important:

Enable IPSG only on an untrusted DHCP snooping port.

Important:

Avaya recommends that you do not enable IPSG on MLT, DMLT and LAG ports.

The following table shows you how IP Source Guard works with DHCP snooping:

Table 6: IP Source Guard and DHCP snooping

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
disabled or enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the binding table entry
enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the binding table entry
enabled	enabled	deletes a binding entry	deletes the IP filter and installs a default filter to block all IP traffic on the port
enabled	enabled or disabled	deletes binding entries when one of the following conditions occurs: • DHCP is released • the port link is down, or the administrator is disabled • the lease time has expired	deletes the corresponding IP Filter and installs a default filter to block all IP traffic
enabled or disabled	enabled	not applicable	deletes the installed IP filter for the port
disabled	enabled	creates a binding entry	not applicable
disabled	enabled	deletes a binding entry	not applicable

IP Source Guard does not support IP and MAC address filters.

Unicast storm control

To control unicast traffic congestion on the switch you can use unicast storm control.

Use unicast storm control to configure a maximum rate, beyond which traffic cannot traverse the switch. This maximum rate is also known as the high water mark. Unicast storm control blocks all unicast traffic, known and unknown, when it exceeds the high water mark.

You can also configure the rate at which traffic can resume, also known as the low water mark. Once the unicast traffic rate drops below the low water mark, all unicast traffic can pass through the switch.

Note:

Regardless of the blocking state of unicast traffic, all broadcast and multicast traffic continues to pass, or forward, unless it is blocked or limited by other means, such as broadcast rate limiting.

How unicast storm control works:

Unicast storm control uses a timed polling mechanism to determine the unicast traffic rate, in packets per second.

The system compares the unicast traffic rate to user-defined thresholds to activate and deactivate a per-port filter.

When traffic rates exceed a high threshold, the system enables the traffic filter and unicast traffic cannot flow through the switch. When the traffic rates drop below the low threshold, the system disables the filter and unicast traffic flows through the switch.

Traps:

Unicast storm control also sends traps to indicate when traffic volumes cross thresholds and it sends repeated traps while the unicast traffic rate remains above the high threshold.

MAC address-based security

You can safeguard your Ethernet networks from unauthorized surveillance and intrusion with the Media Access Control (MAC) address-based security feature, a real-time security system based on Avaya local area network (LAN) access for Ethernet.

You can use MAC address-based security to set up network access control based on the source MAC addresses of authorized stations and to perform the following activities:

- Create a list of up to 10 MAC addresses to filter as:
  - destination addresses (DA)—the system drops all packets containing one of the specified MAC addresses, regardless of the ingress port, source address intrusion, or virtual local area network (VLAN) membership.
  - source addresses (SA)—the system drops all packets containing one of the specified MAC addresses.

    Important:

    Do not use the MAC address for the stack or units in the stack.
- Create a list of up to 448 MAC source addresses. You can populate the list by:
  - Manual configuration — Specify MAC source addresses authorized to connect to the switch or stack.
  - MAC address security learning — Once MAC address learning on ports is enabled, security is temporarily disabled and all MAC source addresses learned are added to the list. Once learning is disabled, security re-enables and only MAC addresses in the list can connect through the port.

- MAC address-based security autolearning — Once autolearning is enabled, the list is populated automatically. For more information, see the following autolearning section.

When you manually configure MAC-based security, you must specify the following:

- Allowed port access - switch ports that can be controlled for each MAC address security association. Configuration options include:
  - NONE
  - ALL
  - single port
  - multiple ports (example: 1/1-4,1/6, 2/9)
- • Optional actions the switch can perform if the software detects a source MAC address security violation. Actions include one, all, or any combination of the following:
  - Send an SNMP trap
  - Turn on DA filtering for the specified source MAC address
  - Disable the specific port

To configure MAC address-based security features you can use either the Avaya Command Line Interface (ACLI) or Enterprise Device Manager (EDM).

MAC address-based security autolearning

To automatically add allowed MAC addresses to the MAC Security Address Table, use the MAC address-based security autolearning feature.

When you use MAC address-based security autolearning you can:

- Specify the number of addresses that can be learned on the ports, to a maximum of 25 addresses for each port. The switch forwards only traffic for those MAC addresses statically associated with a port or those learned with the autolearning process.
- Configure an aging time, in minutes, after which the system refreshes autolearned MAC address entries in the MAC Security Address Table. If you set the aging time value to 0, the entries never age out. To force relearning of entries in the MAC Security Address Table you must reset learning for the port.
- Reset the MAC address table for a port by disabling the security on the port and then enabling it.

When you use MAC address-based security autolearning you cannot modify autolearned MAC addresses in the MAC Security Address Table.

If a port link drops, the system removes the autolearned entries in the MAC Security Address table that are associated with that port.

If you disable autolearning on a port, the system removes all autolearned MAC entries associated with that port in the MAC Security Address Table.

MAC addresses learned with autolearning are not saved to the configuration file — they are dynamically learned by the switch — while MAC Security port configuration, including the aging timer and static MAC address entries, is saved to the switch configuration file.

If a MAC address is already learned on a port and the address migrates to another port, the entry in the MAC Security Address table changes to associate that MAC address with the new port and the system resets the aging timer for the entry.

Note:

This is the opposite of Sticky MAC behavior.

User settings have priority over autolearning. For example, if you associate a static MAC address with a port (which is or is not configured with the autolearning feature) and the same MAC address is learned on a different port, the system does not create an autolearn entry associating that MAC address with the second port in the MAC Security Address Table.

MAC security port lockout

To simplify switch operation and provide protection against improper configurations, you can use MAC Security Port Lockout.

You use MAC security port lockout to exclude specified ports from participating in MAC-based security. You can lock out:

- uplink ports
- MLT ports
- remote-administration ports

MAC Security Port Lockout prevents accidental loss of network connectivity caused by improper MAC security settings.

Sticky MAC address

Sticky MAC address provides a high level of control, and simpler configuration and operation for MAC address security.

You can use the Sticky MAC address feature on either a standalone switch or a stack unit.

With Sticky MAC address, you can secure the MAC address to a specified port, so that if the MAC address moves to another port, the system raises an intrusion event.

When you enable Sticky MAC address, the switch performs the initial autolearning of MAC addresses and can store the automatically learned addresses across switch reboots.

Chapter 4: User access configuration using ACLI

You can use the information in this chapter to configure and manage user access limitations for the Avaya Virtual Services Platform 7000 Series, using the Avaya Command Line Interface (ACLI).

Enabling or disabling password security

Use this procedure to enable or disable password security for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] password security
   ```

Variable definitions

The following table describes the parameters for the **`password security`** command.

Variable	Value
[no]	Disables password security for the switch.

Configuring local RW and RO users accounts

Use this procedure to create or delete local read-write (RW) and read-only (RO) user accounts. The switch supports up to 8 RW and 8 RO user accounts.

Important:

RW and RO user account passwords must be between 8 and 255 alphanumeric characters in length and must include a minimum of the following:

- 2 lower case letters
- 2 upper case letters
- 2 numbers
- 2 special symbols, such as !@#$%^&*()

Passwords are case-sensitive.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To create a local RW or RO user account, enter the following command:

   ```
   username add <WORD> role-name {RO|RW} password
   ```

   The switch prompts you to enter and confirm an alphanumeric password.

   The created RW or RO user account is automatically enabled.

3. To delete a specific user account, enter the following command:

   ```
   no username <LINE>
   ```

   The switch prompts you to confirm if you want to delete the specified password.

Example

Create two RW (User1 and User2) user accounts and two RO (User3 and User4) user accounts.

Note:

In actual command screen output, the `Confirm new password:` prompt replaces the `Enter new password:` prompt after you type your password. For the purpose of this example, the two prompts are displayed one after the other.

```
7024XLS(config)#username add User1 role-name RW password
Enter new password: **********
Confirm new password: **********
7024XLS(config)#
7024XLS(config)#username add User2 role-name RW password
Enter new password: **********
Confirm new password: **********
7024XLS(config)#
7024XLS(config)#username add User3 role-name RO password
Enter new password: **********
Confirm new password: **********
7024XLS(config)#
7024XLS(config)#username add User4 role-name RO password
Enter new password: **********
Confirm new password: **********
```

Delete one RW (User1) user account and one RO (User3) user account.

```
7024XLS(config)#no username User1
The specified user name will be deleted! Continue (y/n) ? y
7024XLS(config)#
7024XLS(config)#no username User3
The specified user name will be deleted! Continue (y/n) ? y
```

Variable definitions

The following table describes the variables for the **username add** and **no username** command parameters.

Variable	Value
<WORD>	Specifies an alphanumeric name for the user account.
{RO|RW}	Specifies the type of user account. Values include: • RO—read-only • RW—read-write
<LINE>	Specifies the alphanumeric name of the user account to delete.

Changing the RO password

Use this procedure to change the existing password for a specific RO user.

About this task

RO users can change their account password in Privileged EXEC ACLI command mode.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   username password
   ```

   The switch prompts you to enter the existing password, then to enter and confirm the new password.

Example

This example shows sample output for the **username password** command.

```
7024XLS#username password
Enter old password:*********
```

```
Enter new password:**********
Confirm new password:**********
```

Configuring password history

Use this procedure to configure the maximum number of passwords stored in the password history table.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   password password-history <3-10>
   ```

Variable definitions

The following table describes the parameters for the **`password password-history`** command.

Variable	Value
<3-10>	Specifies the number of passwords to store in the history table. DEFAULT: 3

Restoring password history to default

Use this procedure to return the number of passwords stored in the password history table to the default value of 3.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default password password-history
   ```

Displaying password history settings

Use this procedure to display the number of passwords currently stored in the password history table.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show password password-history
   ```

Configuring the password expiration period

Use this procedure to configure the period of time after which the password for Telnet or console access to the switch expires.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To set the password expiration period globally for the switch, enter the following command:

   ```
   password aging-time day <1-365>
   ```

3. To restore the password expiration period to default globally for the switch, enter the following command:

   ```
   default password aging-time
   ```

4. To set the password expiration period for a specific user, enter the following command:

   ```
   password aging-time username <WORD> <1-365>
   ```

5. To verify the password expiration period setting, enter the following command:

   ```
   show password aging-time
   ```

Variable definitions

The following table describes the variables for the **`password aging-time day`** and **`password aging-time username`** command parameters.

Variable	Value
<1–365>	Specifies the number of days before the global password expires. Values range from 1 to 365. DEFAULT: 90
<WORD>	Specifies the alphanumeric user name for which to set the password expiration period.
<1–365>	Specifies the number of days before the password for a specific user expires. Values range from 1 to 365. DEFAULT: 90

Enabling or disabling passwords

Use this procedure to enable or disable passwords for Telnet or console access to the switch.

About this task

After the read-only and read-write passwords are set, they can be individually enabled or disabled for the various switch access methods.

When enabled, password security prompts you for a password and the value is hidden.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   cli password {telnet | serial} {none | local | radius | tacacs}
   ```

Variable definitions

The following table describes the parameters for the **`cli password`** command.

Variable	Value
{telnet | serial}	Specifies the password setting for Telnet or the console.
{none | local | radius | tacacs}	Specifies the password type. Values include: • none—disabled, no password • local—use the locally stored password created in *Setting the read-only and write-only passwords*

Variable	Value
	• radius—use RADIUS for AAA services • tacacs—use TACACS+ for AAA services

Related RADIUS commands

During the process of configuring RADIUS authentication, there are three other ACLI commands that can be useful to the process. These commands are:

- **`show radius-server`** — This command displays the current RADIUS server configuration. It has no parameters.
- **`no radius-server`**—This command clears any previously configured RADIUS server settings. It has no parameters.
- **`radius-server password fallback`**—This command enables the password fallback RADIUS option if it was not done when the RADIUS server was configured initially. It has no parameters.

Configuring the maximum number of logon retries

Use this procedure to configure the maximum number of logon retries before a user is locked out of Telnet, SSH, and WEB access to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   telnet-access retry <1-100>
   ```

Variable definitions

The following table describes the parameters for the **`telnet-access retry`** command.

Variable	Value
<1–100>	Specifies the maximum number of logon retry attempts. Values range from 1 to 100. DEFAULT: 3

Configuring the failed logon attempt lockout interval

Use this procedure to configure the period of time that a user is locked out of the switch after the maximum number of logon retry attempts is exceeded.

For information about configuring the maximum allowable number of failed logon attempts, see Configuring the maximum number of logon retries on page 62.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure the failed logon attempt lockout interval, enter the following command:

   ```
   username lockout-time <1-60>
   ```

3. To restore the failed logon attempt lockout interval to default, enter the following command:

   ```
   default username lockout-time
   ```

Variable definitions

The following table describes the parameters for the **`username lockout-time`** command.

Variable	Value
<1-60>	Specifies the time interval (in minutes) that a user is denied access to all password logon interfaces (Telnet, SSH, and WEB), after the predetermined number of logon retry attempts is exceeded. Values range from 1 to 60 minutes. DEFAULT: 1 minute

Unlocking a locked-out user

Use this procedure to unlock switch Telnet, SSH, and WEB access for a user who has exceeded the maximum number of logon retry attempts.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

```
username <username>  unlock
```

Variable Definitions

The following table describes the parameters for the **username <username> unlock** command.

Variable	Value
<username>	Specifies the alphanumeric name of the user account to unlock.

Displaying local user information

Use this procedure to display information about user accounts configured on the local switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display role and status information for all user accounts:

   ```
   show username
   ```

3. Display role and status information for a specific user account:

   ```
   show username <LINE>
   ```

4. Display information for user accounts logged on to the switch using AAA:

   ```
   show who
   ```

Example

The following example displays sample output for the **show username** command.

```
7024XLS#show username

Lockout timeout: 1 min

Username:           RW
-------------------------------------------
Role name:          RW
Enabled:            Yes

Username:           RO
-------------------------------------------
Role name:          RO
Enabled:            Yes

Username:           User1
-------------------------------------------
Role name:          RW
Enabled:            Yes
```

```
Username:           RO2
-------------------------------------------
Role name:          RO
Enabled:            Yes

Username:           Rw2
-------------------------------------------
Role name:          RO
Enabled:            Yes
7024XLS#
```

The following example displays sample output for the **show username <LINE>** command.

```
7024XLS#show username User1

Lockout timeout: 1 min

Username:           User1
-------------------------------------------
Role name:          RW
Enabled:            Yes
7024XLS#
```

The following example displays sample output for the **show who** command.

```
7024XLS#show who
Session  User              Host
-------  ----------------  ---------------------------------------------
7024XLS#
```

Variable definitions

The following table describes the variables for the **show username** command.

Variable	Value
<LINE>	Specifies the alphanumeric name of the user account for which to display information..

Configuring MAC address-based security

You can configure and manage general switch security using MAC address-based security functions.

About this task

You need to protect your network from internal and external attacks. To manage general security tasks, use the following procedure.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
mac-security {auto-learning aging-time <0-65535> | auto-learning
sticky | disable | enable | filtering | intrusion-detect |
intrusion-timer | learning | learning-ports | mac-address-table |
mac-da-filter | security-list | snmp-lock}
```

Variable definitions

Use the following table to help you understand the parameters for the **mac-security** command.

Variable	Value
auto-learning *{aging-time | sticky}*	You can configure either • *aging-time* — configure the interval during which the switch will auto-learn MAC addresses. **RANGE**: 0–65535 seconds. A value of 0 equals forever. • *sticky*— Sets MAC security mode to enable storage of automatically-learned MAC addresses across switch reboots.
disable	Disables MAC address-based security.
enable	Enables MAC address-based security.
filtering *{disable | enable}*	Disables or enables DA filtering for intruder addresses. You can also disable or enable the following **mac-security-filtering** functions: • *learning*— MAC address learning • *learning-ports*— MAC address learning for specific ports • *snmp-lock*— SNMP lock on MAC address security parameters
intrusion-detect *{disable | enable | forever}*	Disables or enables partitioning on intrusion detection. Forever enables permanent partition on intrusion detection. You can also enable or disable the following **mac-security-intrusion-detect** functions: • *filtering*—DA filtering for intruder addresses • *intrusion-timer*— temporary partition time for intrusion detection • *learning*—MAC address learning

Variable	Value
	• *learning-ports*—Modify port participation in MAC address learning • *snmp-lock*—SNMP lock on MAC address security parameters
intrusion-timer *<0–65535>*	Sets temporary partition time, in seconds, for intrusion detection. **RANGE**: 0–65535, 0 = forever
learning *[snmp-lock]*	Disables or enables MAC address learning. You can also disable or enable the following **`mac-security-learning`** function: • *snmp-lock*—SNMP lock on MAC address security parameters
learning-ports *{add [LINE]| LINE [learning | snmp-lock] | remove [LINE]}*	Modify port participation in MAC address learning. • add—add ports • LINE—port list • remove—remove ports
mac-address-table *{address | sticky-address}*	Adds addresses to MAC security address table. • address—specifies an address to add to the MAC security MAC address table in the format H.H.H. • sticky-address—adds a sticky address to the mac-security MAC address table in the format H.H.H.
mac-da-filter *{add | delete }*	Adds MAC DA filtering addresses. Deletes MAC delete filtering addresses.
security-list	Specifies a MAC security list number. **RANGE**: 1–128
snmp-lock	Disables or enables SNMP lock on MAC address security parameters.

Viewing MAC security information

You can view MAC address-based security information to determine the current security configuration, help you plan configuration changes, or troubleshoot issues.

About this task

You can view the MAC security configuration, contents of the MAC address table, MAC DA filtering addresses, MAC security status or ports, and port membership in security lists.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show mac-security {config | mac-address-table | mac-da-filter | port
   | security-lists}
   ```

Variable definitions

You can use the information in the following table to help you understand the **`show mac-security`** command.

Variable	Value
config	Displays the switch or stack MAC security configuration.
mac-address-table [address]	Displays the accessible MAC addresses on each port. • address—displays the accessible port for a specific MAC address
mac-da-filter	Displays the MAC DA filtering addresses.
port [LINE]	Displays the MAC security status or ports. • LINE—list of ports
security-lists [LINE]	Displays port membership of security lists. • LINE—list of security lists

Enabling or disabling IP Manager

Use this procedure to enable or disable the control of Telnet, Web, and SNMP access using IP Manager.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] ipmgr {snmp | source-ip | ssh | telnet | web}
   ```

Variable definitions

The following table describes the parameters for the **ipmgr** command.

Variable	Value
[no]	Disables IP Manager.
snmp	Enables the IP Manager list check for SNMP, including Enterprise Device Manager.
source-ip	Specifies the source IP address from which Telnet, Web, and SNMP access is allowed.
ssh	Enables the IP Manager list check for Secure Shell (SSH) access.
telnet	Enables the IP Manager list check for Telnet access.
web	Enables the IP Manager list check for Web access.

Configuring the IP Manager list

Use this procedure to list specific source IPv4 or IPv6 addresses that can access a switch or stack when IP Manager is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command to list specific source IPv4 addresses:

   ```
   ipmgr source-ip <list ID> <Ipv4addr> [mask <mask>]
   ```

3. Enter the following command to list specific source IPv6 addresses:

   ```
   ipmgr source-ip <list ID> <Ipv6addr/prefix>
   ```

Variable definitions

The following table describes the parameters for the **ipmgr source-ip** command.

Variable	Value
<list ID>	Specifies a value ranging from 1 to 50 that uniquely identifies the IPv4 entry in the IP Manager list. **OR**

Variable	Value
	Specifies a value ranging from 51 to 100 that uniquely identifies the IPv6 entry in the IP Manager list.
<*Ipv4addr*>	Specifies the source IPv4 address from which access is allowed.
mask<*mask*>	Specifies the subnet mask from which access is allowed.
<*Ipv6addr/prefix*>	Specifies the source IPv6 address and prefix from which access is allowed.

Removing IP Manager list entries

Use this procedure to deny access to the switch or stack for specified source IPv4 or IPv6 addresses.

About this task

The command sets both the IP address and mask for the specified entry to 255.255.255.255 for Ipv4 entries and to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for Ipv6 entries. If you do not specify a <*list ID*> value, the command resets the whole list to factory defaults.

Note:

The IPv6 parameter is valid only for switches that support IPv6.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no ipmgr source-ip [<list ID>]
   ```

Variable definitions

The following table describes the parameters for the **`no ipmgr source-ip`** command.

Variable	Value
<*list ID*>	Specifies a value ranging from 1 to 50 that uniquely identifies the Ipv4 entry in the IP Manager list. **OR**

Variable	Value
	Specifies a value ranging from 51 to 100 that uniquely identifies the Ipv6 entry in the IP Manager list. **Note:** The IPv6 parameter is valid only for switches that support IPv6.

Displaying IP Manager settings

Use this procedure to display information about the IP Manager list.

About this task

The command displays the following information:

- If Telnet, SNMP, and Web access are enabled.
- If the IP Manager list is used to control access to Telnet and SNMP.
- The current IP Manager list configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show ipmgr
   ```

Configuring a TACACS+ client

Use this procedure to configure a network switch as a client for a TACACS+ server.

Before you begin

- Configure a TACACS+ server.
- Physically connect the TACACS+ server to your network.

Note:

You can configure and connect a secondary TACACS+ server to your network as a backup for the primary TACACS+ server.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. At the command prompt, enter the following command:

```
tacacs server {host <A.B.C.D>} {key <key>} {secondary-host
<A.B.C.D>} {port <1-65535>}
```

Variable definitions

The following table describes the parameters for the **`tacacs server`** command.

Variable	Value
host<*A.B.C.D*>	Specifies the IP address of the primary TACACS+ server connected to the network.
key<*key*>	Specifies the secret authentication and encryption key, or shared secret, used for all communications between a switch or Network Access Server (NAS) and the TACACS+ server. You must enter the same key as the one defined on the server. You are prompted to confirm the key when you enter it. **Note:** The key parameter is a required parameter when you create a new server entry. The parameter is optional when you are modifying an existing entry.
port<*1–65535*>	Specifies the TCP port for TACACS+ communication. Values range from 1 to 65535. The default value is 49.
secondary-host<*A.B.C.D*>	Specifies the IP address of the secondary TACACS+ server connected to the network. The secondary server is used only if the primary server does not respond.

Disabling a TACACS+ client

Use this procedure to disable the TACACS+ client function for a network switch.

About this task

When you disable the TACACS+ client function for a switch, the IP addresses for the primary and secondary TACACS+ servers are deleted, the secret authentication and encryption key is deleted, and the TCP port configured for TACACS+ is returned to the default value.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter either of the following commands:

   ```
   no tacacs server
   ```

   OR

   ```
   default tacacs server
   ```

Enabling serial TACACS+ services

Use this procedure to enable TACACS+ authentication, authorization, and accounting (AAA) services for users connection to the switch over a serial connection.

Before you begin

- Configure the switch as a TACACS+ client.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   cli password serial tacacs
   ```

Enabling Telnet TACACS+ services

Use this procedure to enable TACACS+ authentication, authorization, and accounting (AAA) services for users connection to the switch over a Telnet connection.

Before you begin

- Configure the switch as a TACACS+ client.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
cli password telnet tacacs
```

Enabling TACACS+ authorization

Use this procedure to enable TACACS+ authorization for the switch.

Note:

TACACS+ authorization is disabled by default.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
tacacs authorization enable
```

Disabling TACACS+ authorization

Use this procedure to disable TACACS+ authorization for the switch.

Note:

TACACS+ authorization is disabled by default.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
tacacs authorization disable
```

Configuring TACACS+ authorization privilege levels

Use this procedure to specify the privilege levels to which TACACS+ authorization applies.

About this task

The TACACS+ authorization privilege levels control which commands can be executed. If a user is assigned a privilege level for which authorization is enabled, TACACS+ authorizes the authenticated user to execute a specific command only if the command is allowed for that privilege level.

Procedure

1. Log on to either the Global or Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:

   ```
   tacacs authorization level {ALL | LINE | NONE}
   ```

Variable definitions

The following table describes the parameters for the **`tacacs authorization level`** command.

Variable	Value
ALL	Enables authorization for all privilege levels.
LINE	Enables authorization for a specific privilege level. Values range from 0 to 15.
NONE	Authorization is not enabled for privilege levels. All users can execute commands available on the switch. *NONE* is the default value.

Enabling or disabling TACACS+ accounting

Use this procedure to enable or disable TACACS+ accounting for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   tacacs accounting {enable | disable}
   ```

Variable definitions

The following table describes the parameters for the **tacacs accounting** command.

Variable	Value
enable	Enables TACACS+ accounting for the switch.
disable	Disables TACACS+ accounting for the switch. TACACS+ accounting is disabled by default.

Configuring the switch TACACS+ level

Use this procedure to select a new TACACS+ level for the switch or use the last configured level.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   tacacs switch {back | level [<1-15>]}
   ```

Variable definitions

The following table describes the parameters for the **tacacs switch** command.

Variable	Value
back	Selects the last configured TACACS+ privilege level.
level*[<1–15>]*	Specifies a new TACACS+ privilege level. Values range from 1 to 15. If you do not enter a level value, the switch uses the default value of 15.

Displaying TACACS+ information

Use this procedure to display the TACACS+ configuration status for the switch

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show tacacs
```

Job aid: sample TACACS+ information display output

The following example displays sample output for the **`show tacacs`** command.

```
7024XLS-PWR(config)#show tacacs
Primary Host: 10.10.10.20
Secondary Host: 0.0.0.0
Port: 49
Key: ***************
TACACS+ authorization is enabled
Authorization is enabled on levels: 1-15
TACACS+ accounting is disabled
```

Configuring switch RADIUS server parameters

Use this procedure to configure a switch to interface with a RADIUS server.

Before you begin

- Configure at least one RADIUS server.
- Physically connect the RADIUS server to your network.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. At the command prompt, enter the following command:

```
[default | no] radius-server [host {<A.B.C.D> | <ipv6addr>}]
[secondary-host {<A.B.C.D> | ipv6addr>}] [key <key>] [password
<fallback>] [port <1-65535>] [timeout <1-60>]
```

3. To configure the RADIUS server authentication type, enter the following command:

```
[default | no] radius-server encapsulation <MS-CHAP-V2>
```

Variable definitions

The following table describes the parameters for the **`radius-server`** command.

Variable	Value
[default | no]	default—restores switch RADIUS server parameters to their default values. no-disables RADIUS server.
host<*A.B.C.D*> | <*ipv6addr*>	Specifies an IPv4 or IPv6 address for the primary RADIUS server. DEFAULT: 0.0.0.0
secondary-host<*A.B.C.D*> | <*ipv6addr*>	Specifies an IPv4 or IPv6 address for a secondary RADIUS server. DEFAULT: 0.0.0.0
key<*key*>	Specifies the secret authentication and encryption key used for all communications between the Network Access Server (NAS) and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
password <*fallback*>	Enables or disables RADIUS password fallback. DEFAULT: Disabled
port<*1–65535*>	Specifies the UDP port the switch uses to interface with the RADIUS server. Values range from 1 to 65535. DEFAULT: 1812
timeout<*1–60*>	Specifies the number of seconds before the switch RADIUS service request times out. RADIUS allows three retries each for the primary and secondary server. DEFAULT: 2
encapsulation <*MS-CHAP-V2*>	Specifies to enable or disable Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAP-V2). MS-CHAP-V2 provides an authenticator-controlled password change mechanism also known as the change RADIUS password function. DEFAULT: disabled **Note:** When you disable MS-CHAP-V2, RADIUS encapsulation is set to password authentication protocol (PAP) by default. PAP is not considered a secure encapsulation. **Note:** Change RADIUS password is available only in secure software builds.

Enabling or disabling RADIUS use management IP

Use this procedure to specify whether or not generated RADIUS requests us the management IP address as the source IP address.

Note:

RADIUS is not supported on the out-of-band management port.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] radius use-management-ip
   ```

Variable definitions

The following table describes the parameters for the **`radius use-management-ip`** command.

Variable	Value
[default]	Sets the RADIUS use management IP configuration to default. DEFAULT: Enabled
[no]	Disables RADIUS use management IP.

Displaying the RADIUS use management IP configuration

Use this procedure to display the configuration status for RADIUS use management IP.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show radius use-management-ip
   ```

Enabling or disabling RADIUS accounting

Use this procedure to enable or disable the recording of management logon activity to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] radius accounting enable
   ```

Variable definitions

The following table describes the parameters for the **`radius accounting enable`** command.

Variable	Value
[default]	Restores RADIUS accounting to the default value. DEFAULT: Disabled
[no]	Disables RADIUS accounting for the switch.

Displaying the switch RADIUS server configuration

Use this procedure to display the configuration status for switch RADIUS server parameters.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show radius-server
   ```

Example

```
7024XLS(config)#show radius-server
RADIUS Global Server
-------------------------------------------------------------
Primary Host           : 0.0.0.0
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 2
Key                    : ***************
Radius Accounting      : Disabled
Radius Accounting Port : 1813
```

```
Other Settings
----------------------------------------------------------------
Password Fallback       : Disabled
RADIUS Encapsulation    : PAP

OR
RADIUS Encapsulation    : MS-CHAP-V2
```

Connecting to a device using Telnet

Use this procedure to establish a connection from the Virtual Services Platform 7000 Series to another Telnet server device in the network.

About this task

The switch does not encrypt data sent over the connection, including passwords.

You can only open four Telnet sessions simultaneously.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command to connect to an IPv4 Telnet server:

   ```
   telnet <Hostname or A.B.C.D> [port <0-65535>]
   ```
3. At the command prompt, enter the following command to connect to an IPv6 Telnet server:

   ```
   telnet <WORD> [port <0-65535>]
   ```

Variable definitions

The following table describes the parameters for the **telnet** command.

Variable	Value
Hostname or A.B.C.D	Specifies the hostname or IPv4 address of the remote Telnet server.
port *<0-65535>*	Specifies the TCP port through which to make the connection.
<WORD>	Specifies the IPv6 address of the remote Telnet server.

Displaying SSH information

Use this procedure to display general SSH settings and information about all active SSH sessions.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   show ssh {download-auth-key | global | session}
   ```

Variable definitions

The following table describes the parameters for the **show ssh** command.

Variable	Value
download-auth-key	Displays authorization key and TFTP server IP address.
global	Displays the SSH configuration for the switch.
session	Displays SSH session information.

Enabling or disabling SSH

Use this procedure to enable or disable Secure Shell (SSH) protocol in a non-secure mode.

When you enable SSH, if the host keys do not exist, they are generated automatically.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] ssh
   ```

Variable definitions

The following table describes the parameters for the **ssh** command.

Variable	Value
[no]	Disables SSH.

Connecting SSH to a host

Use this procedure to establish an SSH connection with a host.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   ssh <A.B.C.D. | host_name> [username <user_name>] [port <0-65535>]
   ```

   Important:

   When SSH connects to a host, if the host is not known to the client, the system displays the following message:

   ```
   The authenticity of host '<host's ip>' can't be established. RSA
   Key with the following SHA256 fingerprint:
   4:90:56:E6:F8:9D:E3:BC:88:10:4F:B4:9B:CD:F4:26:84:6:D6:E1:10:64:
   DD:2E:99:7A:93:27:3B:15:9E:7E. Are you sure you want to continue
   connecting (yes/no)?
   ```

   Important:

   The first time a user connects to a host, the console displays fingerprint and **yes/no** questions for read-write access only. Type `yes` only if the host IP address is reliable (no man-in-the-middle attack happens). After you type `yes`, the system displays the following message:

   ```
   Warning: Permanently added '<host's IP>' (RSA) to the list of
   known hosts.
   ```

Variable definitions

The following table describes the parameters for the **ssh** command.

Variable	Value
<A.B.C.D. | host_name>	Specifies either the host IP address, or the host name.
username*<user_name>*	Specifies an alphanumeric user name.
port *<0–65535>*	Specifies the TCP port number. Values range from 0 to 65535.

Enabling or disabling SSH DSA authentication

Use this procedure to enable or disable user logon with SSH DSA key authentication.

Before you begin

- Disable SSH for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] ssh dsa-auth
   ```

Variable definitions

The following table describes the parameters for the **`ssh rsa-auth`** command.

Variable	Value
[default]	Sets SSH RSA authentication for the switch to the default value. DEFAULT: False (disabled)
[no]	Disables SSH RSA authentication for the switch.

Enabling or disabling SSH RSA authentication

About this task

Use the following procedure to enable SSH RSA authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command to enable the SSH RSA authentication key.

   ```
   [default] [no] ssh rsa-auth
   ```

Variable definitions

The following table describes the parameters for the **ssh rsa-auth** command.

Variable	Value
[default]	Sets SSH RSA authentication for the switch to the default value. DEFAULT: True (enabled)
[no]	Disables SSH RSA authentication for the switch.

Downloading an SSH authentication key from a TFTP or SFTP server

Use this procedure to download an SSH authentication key to the switch from a TFTP or SFTP server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   ssh download-auth-key address <A.B.C.D> | <ipv6_addr> | key-name
   <filename> [<dsa|rsa>]
   ```

Variable definitions

The following table describes the parameters for the **ssh download-auth-key address** command.

Variable	Value
<A.B.C.D>	Specifies an IPv4 address for the TFTP or SFTP server.
<ipv6_addr>	Specifies an IPv6 address for the TFTP or SFTP server.
key-name*<filename>*	Specifies the name of the SSH authentication key file on the TFTP or SFTP server.

Variable	Value
[<dsa|rsa>]	Specifies the type of SSH authentication key file to download, DSA or RSA.

Downloading an SSH authentication key from a USB device

Use this procedure to download an SSH authentication key to the switch from a USB storage device.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   ssh download-auth-key usb [unit <1–8>] key-name <filename> [<dsa|rsa>]
   ```

Variable definitions

The following table describes the parameters for the **`ssh download-auth-key usb`** command.

Variable	Value
key-name*<filename>*	Specifies the name of the SSH authentication key file on the USB storage device.
unit*<1–8>*	In a stack application, this parameter selects the switch in the stack to which the USB storage device is connected.
[<dsa|rsa>]	Specifies the type of SSH authentication key file to download, DSA or RSA.

Downloading an SSH auth key

About this task

Use the following procedure to download an SSH authentication key.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command to download an SSH RSA authentication key.

   ```
   ssh download-auth-key rsa
   ```

   Note:

   When you download an RSA key, the existing key is overwritten. You can no longer use the old key to log onto the switch.

3. Enter the following command to download an SSH DSA authentication key.

   ```
   ssh download-auth-key dsa
   ```

Deleting the SSH DSA authentication key

Use this procedure to delete the SSH DSA authentication key that is currently used on the switch.

Before you begin

- Disable SSH for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no ssh dsa-auth-key
   ```

Deleting an SSH RSA auth key

About this task

Use the following procedure to delete an SSH RSA authentication key.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command to delete the SSH RSA authentication key.

```
no ssh rsa-auth-key
```

Generating an SSH DSA host key

Use this procedure to generate a new SSH DSA host key for the switch.

Before you begin

- Disable SSH for the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ssh dsa-host-key
```

Deleting the SSH DSA host key

Use this procedure to delete the switch SSH DSA host key.

Before you begin

- Disable SSH for the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
no ssh dsa-host-key
```

Generating a new SSH RSA host key

About this task

Use the following procedure to enable default SSH RSA authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command to generate a new SSH RSA host key.

   ```
   ssh rsa-host-key
   ```

Deleting an SSH RSA host key

About this task

Use the following procedure to delete an SSH RSA host key.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command to delete an SSH RSA host key.

   ```
   no ssh rsa-host-key
   ```

Enabling or disabling SSH password authentication

Use this procedure to enable or disable user logon with SSH password authentication.

Before you begin

- Disable SSH for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] ssh pass-auth
   ```

Variable definitions

The following table describes the parameters for the **ssh pass-auth** command.

Variable	Value
[default]	Sets SSH password authentication for the switch to the default value. DEFAULT: True (enabled)
[no]	Disables SSH password authentication for the switch.

Enabling or disabling SSL

Use this procedure to enable or disable Secure Socket Layer for the switch.

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] ssl
   ```

Variable definitions

The following table describes the parameters for the **ssl** command.

Variable	Value
[no]	Disables SSL for the switch.

Creating or deleting a SSL certificate

Use this procedure to create a new SSL certificate or delete a previously existing SSL certificate.

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] ssl certificate
   ```

Result

When you create a new SSL certificate, the following apply:

- The new SSL certificate is used only at the next switch or SSL server reset.
- The new certificate is stored in the NVRAM with the file name SSLCERT.DAT, overwriting any previously existing files with that name.
- The current SSL server operation is not affected.

When you delete an existing SSL certificate, the following apply:

- The certificate in NVRAM is also deleted.
- The current SSL server operation is not affected.

Variable definitions

The following table describes the parameters for the **`ssl certificate`** command.

Variable	Value
[no]	Deletes the existing SSL certificate.

Resetting the SSL server

Use this procedure to reset the SSL server.

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ssl reset
```

Result

When you reset the SSL server with SSL enabled on the switch, the SSL server restarts and initializes with the certificate that is stored in switch NVRAM, and any existing SSL connections are closed.

When you reset the SSL server with SSL disabled on the switch, any existing non-secure connections are also closed, the SSL server restarts, and the non-secure operation resumes.

Displaying the SSL configuration

Use this procedure to display information for the current SSL configuration, or to verify SSL configuration changes.

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show ssl
```

Displaying SSL certificate information

Use this procedure to display the SSL certificate stored in NVRAM and used by the SSL server.

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show ssl certificate
```

Disabling SNMP and Telnet with SSH

Use this procedure to permanently disable SNMP and Telnet management interfaces.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   ssh secure [force]
   ```

Variable definitions

The following table describes the parameters for the **`ssh secure`** command.

Variable	Value
[force]	When you select this variable, the step for confirming whether or not you want to proceed is bypassed.

Selecting a TCP port for SSH daemon

Use this procedure to select a TCP port to use for SSH daemon.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] ssh port <1-65535>
   ```

Variable definitions

The following table describes the parameters for the **`ssh port`** command.

Variable	Value
[default]	Selects the default TCP port for SSH daemon.

Variable	Value
<1-65535>	Specifies a TCP port for SSH daemon. Values range from 1 to 65535.

Generating an SSH Client DSA host key

Use this procedure to generate public and private DSA SSH client host keys for user access authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc dsa-host-key [force]
   ```

Variable definitions

The following table describes the parameters for the **`sshc dsa-host-key`** command.

Variable	Value
[force]	Generates a new DSA host key whether or not there is an existing DSA host key. **Note:** Before you can generate a new DSA host key using the **`sshc dsa-host-key`** command, without the *force* option, you must delete the current DSA host key . If a DSA key exists and you use the command without the *force* option, the system does not generate a new key. The authentication method remains unchanged.

Deleting SSH Client DSA host keys

Use this procedure to delete public or private SSH Client DSA host keys from switch NVRAM.

Note:

When you delete DSA host keys, the DSA authentication state remains unchanged.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no sshc dsa-host-key
   ```

Generating an SSH Client RSA host key

Use this procedure to generate public and private RSA SSH client host keys for user access authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc rsa-host-key [force]
   ```

Variable definitions

The following table describes the parameters for the **`sshc rsa-host-key`** command.

Variable	Value
[force]	Generates a new RSA host key whether or not there is an existing RSA host key. **Important:** Before you can generate a new RSA host key using the **`sshc rsa-host-key`** command, without the *force* option, you must delete the current RSA host key . If a RSA key exists and you use the command without the *force* option, the system does not generate a new key. The authentication method remains unchanged.

Deleting SSH Client RSA host keys

Use this procedure to delete public or private SSH Client RSA host keys from switch NVRAM.

Note:

When you delete RSA host keys, the RSA authentication state remains unchanged.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no sshc rsa-host-key
   ```

Enabling SSH Client authentication

Use this procedure to enable the use of SSH Client password authentication, DSA authentication, or RSA authentication for SFTP file transfers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc authentication {dsa | password | rsa]
   ```

Variable definitions

The following table describes the parameters for the **`sshc authentication`** command.

Variable	Value
dsa	Enables DSA authentication for SSH Client sessions. DEFAULT: True (enabled)
password	Enables password authentication for SSH Client sessions. DEFAULT: False (disabled)
rsa	Enables RSA authentication for SSH Client sessions.

Variable	Value
	DEFAULT: False (disabled)

Important:

When you enable one of the SSH Client authentication parameters, the switch automatically disables the remaining two parameters.

Restoring SSH Client authentication to default

Use this procedure to restore SSH Client authentication for SFTP file transfers to default values.

About this task

The following are the default values for SSH Client authentication parameters:

- *dsa*: True (enabled)
- *password*: False (disabled)
- *rsa*: False (disabled)

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter either of the following commands:

   ```
   default sshc dsa-auth
   ```

   OR

   ```
   no sshc dsa-auth
   ```

Closing an SSH Client session

Use this procedure to close a specific SSH Client session.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc close-session <0-8>
   ```

Variable definitions

The following table describes the parameters for the **sshc close-session** command.

Variable	Value
<0–8>	Specifies the SSH Client session ID.

Displaying SSH client session information

Use this procedure to display active SSH client session information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show sshc sessions
   ```

Job aid: sample SSH session display output

The following example displays sample output for the **show sshc sessions** command.

```
7024XLS#show ssh session

Session  Host
-------  ----------------------------------------------
1        207.179.154.118
```

Configuring the SSH Client DSA key

Use this procedure to configure the SSH Client DSA host key size and generate a new key at the next switch reboot.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. At the command prompt, enter the following command:

```
[default] sshc dsa-key
```

Variable definitions

The following table describes the parameters for the **sshc dsa-key** command.

Variable	Value
[default]	Deletes the existing SSH Client DSA host key and sets the key to the default value at the next switch reboot. DEFAULT: 512 **Important:** You must express the DSA key size value in multiples of 64.

Restoring the SSH Client DSA key to default

Use this procedure to restore the SSH Client DSA key size to the default value of 512 and generate a new key at the next switch reboot.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default sshc dsa-key
   ```

Configuring the SSH Client RSA key

Use this procedure to change the SSH Client RSA key size and generate a new key at the next switch reboot.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc rsa-key {1024-2048}
   ```

Variable definitions

The following table describes the parameters for the **sshc rsa-key** command.

Variable	Value
{1024–2048}	Specifies the range of values (1024 to 2048) that you can change the SSH Client RSA key size to. DEFAULT: 1024 **Important:** The RSA key size value must be expressed in multiples of 128.

Restoring the SSH Client RSA key to default

Use this procedure to restore the SSH Client RSA key size to the default value of 512 and generate a new key at the next switch reboot.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default sshc rsa-key
   ```

Selecting an SSH Client TCP port

Use this procedure to select a TCP port to use for accepting new SSH Client connections.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

```
[default] sshc port <1-65535>
```

Variable definitions

The following table describes the parameters for the **sshc port** command.

Variable	Value
[default]	Restores the TCP port for new SSH Client connections to the default value. DEFAULT: 22
<1–65535>	Specifies a TCP port for new SSH Client connections. Values range from 1 to 65535.

Uploading an SSH Client host key to a TFTP or SFTP server

Use this procedure to upload an SSH Client host key from the switch to a TFTP or SFTP server.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
sshc upload-host-key [address <A.B.C.D> | <ipv6_addr>] key-name
<filename> <dsa |rsa>
```

Variable definitions

The following table describes the parameters for the **sshc upload-host-key** command.

Variable	Value
<A.B.C.D>	Specifies an IPv4 address for the TFTP or SFTP server.
<ipv6_addr>	Specifies an IPv6 address for the TFTP or SFTP server.

Variable	Value
key-name<*filename*>	Specifies the name of the SSH Client host key file to upload to the TFTP or SFTP server.
dsa |*rsa*	Specifies to upload a DSA or RSA authentication key to the TFTP or SFTP server.

Uploading an SSH Client host key to a USB device

Use this procedure to upload an SSH Client host key from the switch to a USB storage device.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   sshc upload-host-key usb [unit <1-8>] key-name <filename> <dsa | rsa>
   ```

Variable definitions

The following table describes the parameters for the **`sshc upload-host-key usb`** command.

Variable	Value
unit<*1–8*>	In a stack application, this parameter selects the switch in the stack to which the USB storage device is connected.
key-name<*filename*>	Specifies the name of the SSH Client host key file to upload to the USB storage device.
<*dsa* | *rsa*>	Specifies to upload a DSA or RSA authentication key to the USB storage device.

Displaying SSH client known host information

Use this procedure to display information about SSH client known hosts configured on the switch.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show sshc known-hosts
```

Note:

The **show sshc known-hosts** command is available only on terminals with Read-Write access.

Clearing SSH Client known hosts

Use this procedure to clear an SSH Client host from the known host table.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. At the command prompt, enter the following command:

```
clear sshc known-host {<A.B.C.D> | <host_name> | <ipv6_address> |
all}
```

Variable definitions

The following table describes the parameters for the **clear sshc known-host** command.

Variable	Value
<A.B.C.D>	Specifies the host IP address.
<host_name>	Specifies the alphanumeric name assigned to the host.
<ipv6_address>	Specifies the host IPv6 address.
all	Clears all hosts from the known host table.

Setting the switch HTTP port

Use this procedure to set the value for the HTTP port that the switch uses for client Web browser requests.

Before you begin

- If the switch is running a secure image, disable SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   http-port {1024-65535}
   ```

Variable definitions

The following table describes the parameters for the **`http-port`** command.

Variable	Value
{1024–65535}	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. DEFAULT: 80

Restoring the switch HTTP port to default

Use this procedure to restore the value for the HTTP port that the switch uses for client Web browser requests to the default value of 80.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default http-port
   ```

Displaying the switch HTTP port value

Use this procedure to display the value for the HTTP port that the switch uses for client Web browser requests.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show http-port
   ```

Setting the switch HTTPS port

Use this procedure to set the value for the HTTPS port that the switch uses for secure client Web browser requests.

Before you begin

- If the switch is running a secure image, disable SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   https-port {1024-65535}
   ```

Variable definitions

The following table describes the parameters for the **`https-port`** command.

Variable	Value
{1024–65535}	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. DEFAULT: 443

Restoring the switch HTTPS port to default

Use this procedure to restore the value for the HTTPS port that the switch uses for secure client Web browser requests to the default value of 443.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   default https-port
   ```

Displaying the switch HTTPS port value

Use this procedure to display the value for the HTTPS port that the switch uses for secure client Web browser requests.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show https-port
   ```

Configuring the Web server for client browser requests

Use this procedure to configure the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

Before you begin

- Enable SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] https-only
   ```

Result

Employing the **`https-only`** root command enables the HTTPS only feature and the Web server responds to secure (HTTPS) client browser requests only.

Variable definitions

The following table describes the parameters for the **`https-only`** command.

Variable	Value
[default]	Restores the HTTPS only function to the default value. DEFAULT: Enabled
[no]	Disables the HTTPS only function and the Web server responds to both secure (HTTPS) and non-secure (HTTP) client browser requests.

Displaying the Web server client browser request status

Use this procedure to display whether the Web server is configured to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

Before you begin

- Enable SSL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   show https-only
   ```

Enabling or disabling IP Source Guard

Use this procedure to enable or disable the filtering of clients with invalid IP addresses on a switch port, or range of ports.

Before you begin

- Enable Dynamic Host Control Protocol (DHCP) snooping globally for the switch.
- Ensure ports are members of a Virtual LAN (VLAN) that has DHCP snooping and dynamic Address Resolution Protocol (ARP) inspection enabled.
- Ensure that DHCP snooping and dynamic ARP inspection are set to *untrusted* for the ports
- Ensure that the **bsSourceGuardConfigMode** MIB object exists.

This MIB object is used to control the IP Source Guard mode on an interface.

- Ensure that the following application is not enabled on the switch:
  - IP Fix

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] ip verify source interface <interface_type>
   [portlist]
   ```

Variable definitions

The following table describes the parameters for the **`ip verify source interface`** command.

Variable	Value
[default]	Sets IP Source Guard for the port or ports to the default value. DEFAULT: Disabled
[no]	Disables IP Source Guard for the port or ports.
<interface_type>	Specifies the type of interface associated with the ports.
[portlist]	Specifies a port or list of ports for which to enable or disable IP Source Guard. **Note:** If you do not include this optional parameter when you use the *[default]* or *[no]* option with the **`ip verify source interface`** command, IP Source Guard is disabled for all ports that meet the required prerequisites.

Displaying IP Source Guard interface configuration

Use this procedure to display the IP Source Guard configuration status for switch interface ports.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show ip verify source [interface {<interface_type> <portlist>}]
   ```

Variable definitions

The following table describes the parameters for the **`show ip verify source`** command.

Variable	Value
interface	Specifies to display the IP Source Guard configuration status for a specific interface.
<interface_type>	Specifies the interface type.
<portlist>	Specifies an individual port or list of ports.

Enabling or disabling unicast storm control

Use this procedure to configure unicast storm control to block all known and unknown unicast traffic once a user-configurable threshold (high water mark) is crossed and then allow all unicast traffic to pass/forward once it has dropped below a user configurable (low water mark) threshold.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] storm-control unicast [enable] [high-watermark <range>] [low-watermark <range>] [trap-send-interval <range>] [poll-interval <range>]
   ```

Variable definitions

The following table describes the parameters for the **`storm-control unicast`** command.

Variable	Value
[no]	Disables unicast storm control

Variable	Value
[enable]	Enables unicast storm control DEFAULT: disabled
high-watermark *<11–100000000>*	Specifies the high watermark value in packets per second. RANGE: 11 to 100,000,000 pps
low-watermark *<10–99999999>*	Specifies the low watermark value in packets per second. RANGE: 10 to 99,999,999 pps
poll-interval *<5–300>*	Specifies the time period in seconds over which the packet rate is computed. RANGE: 5 to 300 seconds
trap-send-interval *<0–1000>*	Specifies the number of polling cycles between sending of traps. A trap-send-interval of zero (0) means disabled (high watermark traps will not be repeated).

Chapter 5: User access configuration using EDM

This chapter describes the procedures to manage and configure security on using Enterprise Device Manager (EDM).

Configuring the Web and Telnet password

Use the following procedure to configure a password for Web and Telnet access to a stack, or standalone switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Web/Telnet/Console**.
3. In the work area, click the **Web/Telnet** tab.
4. Click the arrow on the **Web/Telnet Password Type** field.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Password** field.
7. Type the same password for read-only access in the **Re-enter to verify** field.
8. Type the password for read-write access in the **Read-Write Password** field.
9. Type the same password for read-write access in the **Re-enter to verify** field.
10. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with configuring the web and telnet passwords.

Variable	Value
Web/Telnet Password Type	Specifies the type of the password to use. Values include: • none-disables the password. • Local Password — uses the locally defined password for Web and Telnet access. • RADIUS Authentication — uses RADIUS password authentication for Web and Telnet access.
Read-Only Password	Specifies the read-only password for stack or switch access.
Read-Write Password	Specifies the read-write password for stack or switch access.

Configuring the console password

Use the following procedure to configure a password for serial console access to a stack, or standalone switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Web/Telnet/Console**.
3. In the work area, click the **Console Password** tab.
4. Click the arrow on the **Console Password Type** field.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Password** field.
7. Type the same password for read-only access in the **Re-enter to verify** field.
8. Type the password for read-write access in the **Read-Write Password** field.
9. Type the same password for read-write access in the **Re-enter to verify** field.
10. On the toolbar, click **Apply**.

Variable defintions

The following table describes the variables of the console password

Variable	Value
Console Password Type	Specifies the type of password to use. Values include: • none — disables the password. • Local Password — uses the locally defined password for serial console access. • RADIUS Authentication — uses RADIUS authentication for serial console access.
Read-Only Password	Specifies the read-only password for stack or switch access.
Read-Write Password	Specifies the read-write password for stack or switch access.

Configuring MAC security

You can configure and manage general switch security on the MAC security tab in EDM.

About this task

You need to protect your network from internal and external attacks. To manage general security tasks, use the following procedure.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. On the **MAC Security** tab, configure general switch security parameters as required.
4. On the toolbar, click **Apply**.

Variable definitions

Use the information in the following table to help you configure general switch security.

Variable	Value
AuthSecurityLock	If this parameter is listed as locked, the agent refuses all requests to modify the security configuration. Entries also include: • other • notlocked **DEFAULT**: notlocked
AuthCtlPartTime	Indicates the duration of time for port partitioning in seconds.

Variable	Value
	Value ranges between 0 and 65535 seconds. **DEFAULT**: 0 (zero). When the value is zero, port remains partitioned until you manually re-enable it.
SecurityStatus	Indicates whether or not the switch security feature is enabled. **DEFAULT**: disabled
SecurityMode	Specifies mode of switch security. Entries include: • macList—Indicates that the switch is in the MAC-list mode. It is possible to configure more than one MAC address for each port. • autoLearn—Indicates that the switch learns the MAC addresses on each port as allowed addresses of that port. **DEFAULT**: macList.
SecurityAction	Specifies the actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified applies to all ports of the switch. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: • noAction—Port does not have security assigned to it, or the security feature is turned off. • partitionPort—Port is partitioned. • partitionPortAndsendTrap—Port is partitioned and traps are sent to the trap receive station. • daFiltering—Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap—Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. • partitionPortAnddaFiltering—Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap—Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. **Note:** da — destination address
CurrNodesAllowed	Specifies the current number of entries of the nodes allowed in the AuthConfig tab. **DEFAULT**: 0 (zero)

Variable	Value
MaxNodesAllowed	Specifies the maximum number of entries of the nodes allowed in the AuthConfig tab. **DEFAULT**: 448
PortSecurityStatus	Specifies the set of ports for which security is enabled.
PortLearnStatus	Specifies the set of ports where auto-learning is enabled.
CurrSecurityLists	Specifies the current number of Security list entries on the SecurityList tab. **DEFAULT**: 0 (zero)
MaxSecurityLists	Specifies the maximum number of Security List entries on the SecurityList tab. **DEFAULT**: 128
AutoLearningAgingTime	Specifies the MAC address age-out time, in minutes, for the auto-learned MAC addresses. A value of zero (0) indicates that the address never ages out. **DEFAULT**: 60
AutoLearningSticky (sticky-mac)	Specifies whether the sticky MAC feature is enabled. **Important:** You must disable autolearning before you enable **AutoLearningSticky**. **DEFAULT**: disabled
SecurityLockoutPortList	Controls the list of ports excluded from MAC-based security. **Important:** You must disable autolearning before you change the **SecurityLockoutPortList**.

Modifying a MAC Security list

You can make changes to security lists, as required, to help manage security for your system.

About this task

Use this procedure to manage security list port members as follows:

- add ports
- delete all ports
- delete specific ports

Procedure

1. From the navigation tree, double-click **Security**.

2. In the Security tree, double-click **MACSecurity**.
3. In the work area, click the **SecurityList** tab.
4. To add ports, do the following:
   a. Click the **Insert** button. The Insert Security List dialog appears.
   b. Type a number for the security list in the **SecurityListIndx** box.
   c. Do one of the following:

      Click the **SecurityListMembers** ellipsis [...] and select ports to add to the security list.

      Click **All** to select all ports.
   d. Click **OK**.
   e. Click **Insert**.
5. To remove specific existing port members from a security list, do the following:
   a. On the **SecurityList** tab, double-click the **SecurityList Members** box.
   b. Deselect security list port members as required.
   c. Click **OK**.
   d. Click **Apply**.
6. To remove all existing port members from a security list, do the following:
   a. Click the **SecurityListMembers** box.
   b. Click **Delete**.
   c. Click **Yes**.

Variable definitions

Use the information in the following table to help you manage security lists.

Name	Description
SecurityListIndx	Indicates the numerical identifier for a security list. Values range from 1–128.
SecurityListMembers	Describes the security list port members.

Modifying the MAC AuthConfig list

You can add or remove entries from a list of boards, ports, and MAC addresses that have the security configuration.

About this task

You cannot modify entries whose source is autoLearn.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **MACSecurity**
3. In the work area, click the **AuthConfig** tab.
4. To add entries, do the following:
   a. On the toolbar, click **Insert**. The insert AuthConfig dialog box appears.
   b. Type a value in the **BrdIndx** box.
   c. Type a value in the **PortIndx** box.
   d. Type a value in the **MACIndx** box.
   e. Do one of the following:

      Select the **AutoLearningSticky** box to enable Sticky MAC address.

      Clear the **AutoLearningSticky** check box to disable Sticky MAC address.
   f. Do one of the following

      Click the **AccessCtrlType** button to allow a MAC address on multiple ports.

      Click the **AccessCtrlType** button to clear the selection.
   g. Type a value in the **SecureList** box.
   h. Click **Insert**.
5. To delete entries, do the following:
   a. On the **AuthConfig** tab, select a list entry.
   b. Click **Delete**.
   c. Click **Yes**.

Variable definitions

Use the information in the following table to help you modify the AuthConfig list.

Name	Description
BrdIndx	Indicates the index of the board. This corresponds to the unit. The range is 1–8. **Important:** If you specify a BrdIndx, the SecureList field is 0.

Name	Description
PortIndx	Indicates the index of the port.The range is 1–98. **Important:** If you specify a PortIndx, the SecureList field is 0.
MACIndx	Indicates the index of MAC addresses that are designated as allowed (station) or not-allowed (station).
AccessCtrlType	Displays the node entry node allowed. A MAC address can be allowed on multiple ports.
SecureList	Indicates the index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, this field can also have the value of zero. The range is 0–128. The corresponding MAC address of this entry is allowed or blocked on all ports of this port list.
Source	Indicates the method used by the MAC security and MAC address tables to learn MAC addresses. Values include: • **Static** • **Sticky** • **AutoLearn**
Lifetime	Indicates the time period before the system automatically deletes an AuthConfig entry.

Configuring MAC Address AutoLearn

You can configure MAC Address automatic learning properties for switch ports.

Before you begin

- Ensure that the port is not a member of PortLearnStatus

About this task

You cannot enable AutoLearn if the port is a member of PortLearnStatus (on the Mac Security tab).

If you disable AutoLearn, all automatically learned MAC addresses are removed from the port(s).

Procedure

1. From the navigation tree, double-click **Security**

2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AutoLearn** tab.
4. Double-click the Enabled cell for a port and do one of the following:
   - Select **true** to enable automatic learning on the port.
   - Select **false** to disable automatic learning on the port.
5. Double-click the **MaxMacs** cell for a port.
6. Type a value between `1` and `25`.
7. Click **Apply**.

Variable definitions

You can use the information in the following table to help you configure MAC Address AutoLearn.

Name	Description
Unit	Identifies the unit.
Port	Identifies the port.
Enabled	Enables or disables automatic learning on a port. The choices are: • true (enabled) • false (disabled) **DEFAULT**: false
MaxMacs	Defines the maximum number of MAC addresses that the port can learn. **RANGE**: 1–25 **DEFAULT**: 2

Viewing MAC AuthStatus information

You can view authorization status information for boards and port.

Before you begin

- Configure the MAC security parameters on the Mac Security tab

About this task

Use the following procedure to display authorization status information that includes actions the system takes when an unauthorized station is detected and the current security status of a port.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AuthStatus** tab to view the status information.

Variable definitions

You can use the information in the following table to help you understand and use the contents of the AuthStatus tab.

Name	Description
AuthStatusBrdIndx	Displays the index of the board. The index corresponds to the index of the slot that contains the board if the index is >0.
AuthStatusPortIndx	Displays the index of the port on the board. This index corresponds to the index of the last manageable port on the board if the index is >0.
AuthStatusMACIndx	Displays the index of the MAC address on the board. This value corresponds to the index of the MAC address on the port if the index is >0.
CurrentAccessCtrlType	Displays whether the node entry is *node allowed* or *node blocked* type.
CurrentActionMode	Displays a value that represents the type of information contained, including: • noAction—Port does not have security assigned to it, or the security feature is turned off. • partitionPort—Port is partitioned. • partitionPortAndsendTrap—Port is partitioned and traps are sent to the trap receive station. • Filtering—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. • FilteringAndsendTrap—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. • sendTrap—A trap is sent to trap receive stations. • partitionPortAnddaFiltering—Port is partitioned and will filter out the frames with the destination

Name	Description
	address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap—Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations.
CurrentPortSecurStatus	Displays the security status of the current port, including: • notApplicable—the port is disabled. • portSecure—the port is in a normal state • portPartition—the port is partitioned

Viewing MAC AuthViolation information

You can display a list of boards and ports where network violations have occurred.

Before you begin

- Configure MAC Security on your switch

About this task

Use the following procedure to view access violation information about boards and ports.

You can also display the identity of MAC addresses that have attempted unauthorized network access.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AuthViolation** tab.

Variable definitions

You can use the information in the following table to help you understand the contents of the AuthViolation tab.

Name	Description
BrdIndx	Indicates the index of the board. This corresponds to the slot containing the board. The index is 1 where it is not applicable.

Name	Description
PortIndx	Indicates the index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	Indicates the MAC address of the device attempting unauthorized network access (MAC address-based security).

Viewing MAC Violation information

You can display a list of boards and ports where network access violations have occurred.

Before you begin

- Configure MAC Security on your switch

About this task

Use the following procedure to display a list of boards and ports where network access violations have occurred.

You can also display the identity of MAC addresses that have attempted unauthorized access.

Procedure

1. From the navigation tree, double-click **Security**.
2. From the Security tree, double-click **MAC Security.**
3. In the work area, click the **MacViolation** tab.

Variable definitions

Use the information in the following table to help you understand the contents of the MacViolation tab.

Name	Description
Address	Indicates the MAC address of the device attempting unauthorized network access (MAC address-based security).
Brd	Indicates the index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable.
Port	Indicates the index of the port on the board. This corresponds to the port on which a security violation was seen.

Configuring SSH

Use this procedure to configure Secure Shell (SSH) protocol for providing secure access to ACLI interface.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the SSH/SSL work area, click the **SSH** tab.
4. Configure SSH as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the SSH configuration.

Variable definitions

Variable	Value
Enable	Enables, disables, or selects secure mode for SSH authentication. Values include: • **false**: Disables SSH. • **true**: Enables SSH. • **secure**: Selects secure mode.
Version	Displays the SSH version.
Port	Specifies the SSH connection port. Values range from 1 to 65535. DEFAULT: 22
Timeout	Specifies the SSH connection timeout in seconds. Values range from 1 to 120 seconds. DEFAULT: 60
KeyAction	Specifies the SSH key action. Values include: • **generateDsa**: Generates a DSA key. • **generateRsa**: Generates a RSA key. • **deleteDsa**: Deletes a DSA key. • **deleteRsa**: Deletes a RSA key.
RsaAuth	Enables or disables SSH RSA authentication.
DsaAuth	Enables or disables SSH DSA authentication.
PassAuth	Enables or disables SSH password authentication.
RsaAuthKeyName	Indicates the authentication key name.

Variable	Value
DsaAuthKeyName	Indicates the authentication key name.
RsaHostKeyStatus	Indicates the current status of the SSH RSA host key. Values include: • **noSuchInstance_OID** • **notGenerated** • **generated** • **generating**
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key. Values include: • **noSuchInstance_OID** • **notGenerated** • **generated** • **generating**
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server. Values include: • **ipv4** • **ipv6**
TftpServerInetAddress	Specifies the IP address of the TFTP server for all TFTP operations.
TftpFile	Specifies the name of file for the TFTP transfer.
TftpAction	Specifies the action for the TFTP transfer. Values include: • **downloadSshDSAPublicKeys** • **deleteSshDsaAuthKey** • **downloadSshRsaPublicKeys** • **deleteSshRsaAuthKey**
TftpResult	Displays the result of the last TFTP action request.
SshAuthKeyFilename	Specifies the name of the SSH authentication key file to download.
UsbTargetUnit	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 0 to 10. DEFAULT: 0 • **1 to 8**: Specifies a USB port in a switch stack. • **9**: Specifies a standalone switch. • **0**: Specifies to use a TFTP server instead of a USB port.

Variable	Value
	• **10**: Specifies to use a SFTP server instead of a USB port.
Action	When **DnldSshAuthKeyFromUsb** is selected, the SSH authentication key is downloaded using the USB port.
Status	Indicates the status of the latest SSH authentication key download using the USB port. Values include the following: • **other**: No action was taken since the switch boot up. • **inProgress**: The authentication key download is in progress. • **success**: The authentication key download completed successfully. • **fail**: The authentication key download failed.
RsaKeySize	Indicates the SSH RSA key size. Values range from 1024 to 2048. Default: 1024.

Displaying SSH sessions information

Use the following procedure to display currently active SSH sessions.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the SSH/SSL work area, click the **SSH Sessions** tab.

Variable definitions

Variable	Value
SshSessionInetAddressType	Indicates the type of IP address of the SSH client that opened the SSH session.
SshSessionInetAddress	Indicates the IP address of the SSH client that opened the SSH session.

Configuring an SSH Client

Use this procedure to configure and manage a Secure Shell (SSH) Client.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the SSH/SSL work area, click the **SSHC/SFTP** tab.
4. Configure SSH Client as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the SSH Client configuration.

Variable definitions

Variable	Value
KeyAction:	Specifies the action to take for the SSH Client host key. Values include: • **generateDsa**: Generates a DSA host key for the SSH Client. • **generateRsa**: Generates an RSA host key for the SSH Client. • **deleteDsa**: Deletes the SSH Client DSA host key. • **deleteRsa**: Deletes the SSH Client RSA host key. • **generateDsaForce**: Creates a new DSA key, even in the presence of an existing DSA key. • **generateRsaForce**: Creates a new RSA key, even in the presence of an existing RSA key.
KeyFileName:	Specifies the a SSH Client host key file name.
TftpAction:	Specifies the type of SSH Client authentication key to upload using TFTP. Values include: • **uploadSshcDsaAuthKey**: Uploads a DSA SSH Client authentication key using TFTP. • **uploadSshcRsaAuthKey**: Uploads an RSA SSH Client authentication key using TFTP.
TftpServerInetAddressType:	Indicates the type of address stored in the TFTP server. Values include: • **ipv4** • **ipv6**

Variable	Value
TftpServerInetAddress:	Specifies the IP address of the TFTP server for all TFTP operations.
UsbAction:	Specifies the type of SSH Client authentication key to upload using USB. Values include: • **uploadSshcDsaAuthKey**: Uploads a DSA SSH Client authentication key using USB. • **uploadSshcRsaAuthKey**: Uploads an RSA SSH Client authentication key using USB.
UsbTargetUnit:	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 0 to 10. DEFAULT: 0 • **1 to 8**: Specifies a USB port in a switch stack. • **9**: Specifies a standalone switch. • **0**: Specifies to use a TFTP server instead of a USB port. • **10**: Specifies to use a SFTP server instead of a USB port.
DsaKeySize:	Specifies the DSA key size. Values range from 512 to 1024.
RsaKeySize:	Specifies the RSA key size. Values range from 1024 to 2048.
DsaHostKeyStatus:	Indicates the current status of the SSH Client DSA host key. Values include: • **notGenerated** • **generated** • **generating**
RsaHostKeyStatus:	Indicates the current status of the SSH Client RSA host key. Values include: • **notGenerated** • **generated** • **generating**
SFTP	
Port:	Specifies the TCP port number for the SFTP file transfer. Values range from 1 to 65535.
DsaAuthentication	When selected, enables SFTP DSA authentication for SSH Client (default).
RsaAuthentication	When selected, enables SFTP RSA authentication for SSH Client.

Variable	Value
PasswordAuthentication	When selected, enables SFTP password authentication for SSH Client.
SftpServerInetAddressType:	Indicates the type of address stored in the SFTP server. Values include: • **ipv4** • **ipv6**
SftpServerInetAddress:	Specifies the IP address of the SFTP server.
UserName:	Specifies the user name for connecting to the SFTP server.
SftpServerPassword:	Specifies a password for the SFTP server.
Confirm SftpServerPassword:	Confirms the password entered for the SFTP server.

Configuring SSL

Use this procedure to provide your network with a secure Web management interface to configure Secure Socket Layer (SSL).

Before you begin

- The switch must be running a secure image to support SSL.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSL** tab.
4. Configure SSL parameters as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the SSL configuration.

Variable definitions

The following table describes the variables associated with configuring the Secure Socket Layer.

Variable	Value
Enabled	Enables or disables SSL.
CertificateControl	Creates a new SSL certificate or deletes a previously existing SSL certificate.

Variable	Value
	When you create a new SSL certificate, the following apply: • The new SSL certificate is used only at the next switch or SSL server reset. • The new certificate is stored in the NVRAM with the file name SSLCERT.DAT, overwriting any previously existing files with that name. • The current SSL server operation is not affected. When you delete an existing SSL certificate, the following apply: • The certificate in NVRAM is also deleted. • The current SSL server operation is not affected.
CertificateExists	Indicates if a valid SSL certificate exists in NVRAM. Values include: • true—a valid SSL certificate does exist in NVRAM. • false—a valid SSL certificate does not exist in NVRAM
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate. Values include: • inProgress—the operation is not yet completed. • success—the operation is complete. • failure—the operation failed. • other—the status is not available.
ServerControl	Resets the SSL server. **Important:** You cannot reset the SSL server while creating the SSL certificate.

Configuring RADIUS globally

Use the following procedure to configure RADIUS security for the switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **RADIUS**.
3. In the work area, click the **Globals** tab.

4. Configure RADIUS security for the switch as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the global RADIUS security configuration.

Variable definitions

Variable	Value
UseMgmtIp	Select UseMgmtIp to allow RADIUS to use the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
Reachability	Specifies the RADIUS server reachability mode. Values include: • use-radius—uses dummy RADIUS requests to determine reachability of the RADIUS server. • use-icmp—uses ICMP packets to determine reachability of the RADIUS server (default).
ReachabilityUserName	Specifies a user identification name for RADIUS reachability.
ReachabilityPassword	Specifies a user password for RADIUS reachability.
Confirm ReachabilityPassword	Re-enter the user password for verification.
EncapsulationProtocol	Specifies the RADIUS encapsulation protocol. Values include: • pap — Password Authentication Protocol • ms-chap-v2 — Microsoft Challenge Handshake Authentication Protocol Version 2

Configuring the global RADIUS server

Use this procedure to configure a Global RADIUS server to process client requests for network access.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **RADIUS**.
3. In the RADIUS work area, click the **RADIUS Server** tab.
4. Configure the global RADIUS server as required.

5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the RADIUS Server configuration.

Variable definitions

The following table describes the variables associated with the Global RADIUS server.

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary Global RADIUS server. Values include ipv4, and ipv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address for the primary Global RADIUS Server. The default address is 0.0.0.0. **Important:** An IPv4 address value of 0.0.0.0 indicates that a primary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary Global RADIUS Server is not configured.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS Server. Values include ipv4, and ipv6.
SecondaryRadiusServer	Specifies the IP address for the secondary Global RADIUS Server. The default address is 0.0.0.0. The secondary Global RADIUS Server is used only if the primary Global RADIUS Server is unavailable or unreachable. **Important:** An IPv4 address value of 0.0.0.0 indicates that a secondary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured.
RadiusServerUdpPort	Specifies the UDP port number for clients to use when trying to contact the Global RADIUS Server at the corresponding Global RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the Global RADIUS Server. The

Variable	Value
	default is 2 Seconds. Values range from 1 to 60 seconds.
SharedSecret(Key)	Specifies a new value for the Global RADIUS Server shared secret key, to a maximum of 16 characters.
ConfirmedSharedSecret(Key)	Confirms the value typed in the shared secret key box. If you do not change the Global RADIUS Server shared secret key, you do not have to type a value in this box.

Configuring RADIUS use management IP

Use the following procedure to enable or disable RADIUS use of management IP.

Note:

RADIUS is not supported on the out-of-band management port.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **RADIUS.**.
3. In the work area, click the **Globals** tab.
4. Select the **RadiusUseMgmtIP** field to enable or disable RADIUS use of management IP.
5. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
RadiusUseMgmtIp	Controls whether RADIUS uses the IP address of system management as the source address for RADIUS requests.
RadiusPasswordFallbackEnabled	Enables or disables RADIUS password fallback.

Enabling or disabling RADIUS accounting

Use the following procedure to enable or disable RADIUS accounting.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **RADIUS**.
3. In the RADIUS work area, click the **RADIUS Accounting** tab.
4. To enable RADIUS Accounting, select the **RadiusAccountingEnabled** check box.

   OR

   To disable RADIUS Accounting, clear the **RadiusAccountingEnabled** check box.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the RADIUS Accounting configuration.

Variable definitions

Variable	Value
RadiusAccountingEnabled	Enables or disables RADIUS Accounting. DEFAULT: Disabled
RadiusAccountingPort	Indicates the port used for RADIUS Accounting. DEFAULT: 1813

Configuring TACACS+ services

Use the following procedure to configure a TACACS+ services.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **TACACS+**.
3. In the TACACS+ work area, click the **Globals** tab.
4. In the Globals section, configure the parameters as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the TACACS+ configuration.

Variable definitions

The following table describes the variables associated with configuring TACACS+ services.

Variable	Value
Accounting	Enables or disables TACACS+ accounting.
Authentication	Indicates the authentication status.
AuthorizationEnabled	Enables or disables TACACS+ authorization.
AuthorizationLevels	Indicates the TACACS+ authorization level.

TACACS+ server management

You can use the information in this section to add a TACACS+ server to or remove a TACACS+ server from a network.

Adding a TACACS+ server

Use the following procedure to add a new TACACS+ server to the network.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **TACACS+**.
3. In the TACACS+ work area, click the **TACACS+ Server** tab.
4. On the toolbar, click **Insert**.
5. Configure the new TACACS+ server as required.
6. Click **Insert**.
7. On the toolbar, you can click **Refresh** to verify the TACACS+ server configuration.

Variable definitions

Variable	Value
AddressType	Specifies the type of IP address used on the TACACS+ server.
Address	Indicates the IP address of the TACACS+ server in use.
PortNumber	Indicates the TCP port on which the client establishes a connection to the server.
Key	Indicates the secret key to be shared with this TACACS+ server. Key length zero indicates no encryption is used.

Variable	Value
Priority	Determines the order in which the TACACS+ servers are used. Available options are— primary or secondary.

Deleting a TACACS+ server

Use the following procedure to delete a TACACS+ server from the system.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **TACACS+**.
3. In the TACACS+ work area, click the **TACACS+ Server** tab.
4. In the table, select the TACACS+ server entry you want to delete.
5. On the toolbar, click **Delete**.
6. Click **Yes** to confirm.
7. On the toolbar, you can click **Refresh** to verify the TACACS+ server configuration.

Configuring a port-based IP Source Guard

Use this procedure to configure IP Source Guard to enable or disable a higher level of security on a port or ports.

Important:

The IP addresses are obtained from DHCP snooping binding table entries defined automatically in the port. A maximum 10 IP addresses from the binding table are allowed and the rest are dropped.

Before you begin

About this task

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is enabled globally enabled. See this document for more information on DHCP snooping.
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- A minimum of 10 rules are available on the port.

- The bsSourceGuardConfigMode MIB object exists. This MIB object controls the IP Source Guard mode on an interface.
- The following applications are not enabled:
  - IP Fix

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-port** tab.
4. In the table, double-click the cell under the column heading **Mode** for a port.
5. Select a value (enabled or disabled) to enable or disable IP Source Guard.
6. In the toolbar, click **Refresh** to update the IP Source Guard-port dialog box display.

Variable definitions

Variable	Value
Port	Identifies the port number
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Filtering IP Source Guard addresses

Use this procedure to filter IP Source Guard addresses to display IP Source Guard information for specific IP addresses.

Important:

Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs, which have DHCP snooping enabled. If this happens, traffic sending can be interrupted for some clients. Avaya recommends that IP Source Guard not be enabled on trunk ports.

Important:

The IP addresses are obtained from DHCP snooping binding table entries defined automatically in the port. A maximum 10 IP addresses from the binding table are allowed and the rest are dropped.

Before you begin

About this task

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is enabled globally. See this document for more information on DHCP snooping
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- A maximum of 10 rules are available on the port.
- The bsSourceGuardConfigMode MIB object exists.

  This MIB object is used to control the IP Source Guard mode on an interface.
- The following applications are not enabled:
  - IP Fix

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-addresses** tab.
4. In the table, select a record.
5. On the toolbar, click **Filter**. The IP Source Guard-addresses — Filter tab appears.
6. Configure the parameters as required.
7. Click **Filter**.

Variable definitions

The following table describes the parameters for **IP Source Guard-addresses**.

Variable	Value
Port	Indicates the port number.
Type	Indicates the type of interface associated with the ports.
Address	Indicates the IP address.
Source	Indicates the IP source.

Chapter 6: SNMP configuration using ACLI

You can use the information in this chapter to monitor devices running software that supports the retrieval of SNMP information, using the Avaya Command Line Interface (ACLI).

Displaying the SNMP server configuration

Use this procedure to display SNMP server configuration information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show snmp-server [community | host | notification-control | notify-
   filter | user | view]
   ```

Variable definitions

The following table describes the parameters for the **`show snmp-server`** command.

Variable	Value
host	Displays the SNMP trap destination..
notification-control	Displays the SNMP notification control table.
notify-filter	Displays the SNMP notify filter configuration.
user	Displays the SNMP users, including views accessible to each user.
view	Displays SNMP views.

Enabling SNMP server access

Use this procedure to enable SNMP server access to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server enable
   ```

Disabling SNMP server access

Use this procedure to disable SNMP server access to the switch.

Important:

If you disable SNMP server access to the switch, you cannot use Enterprise Device Manager (EDM) for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server disable
   ```

   OR

   ```
   no snmp-server
   ```

Configuring read or write SNMP server community access

Use this procedure to configure a single read-only or a single read-write community string for SNMPv1 and SNMPv2c access.

About this task

A community configured using this command does not have access to any of the SNMPv3 MIBs. The community strings created by this command are controlled by the SNMP Configuration screen in the console interface. These community strings have a fixed MIB view.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
[default] snmp-server community [ro|rw]
```

Variable definitions

The following table describes the parameters for the **`snmp-server community`** command.

Variable	Value
[default]	Restores the read-only (ro) community to **Public**, or the read-write (rw) community to **Private**.
ro|rw	Specifies read-only (ro) or read-write (rw) access for an SNMP server community. When you select either *ro* or *rw* access for an SNMP community, the switch prompts you to enter and confirm a community string. If you do not specify read-only or read-write access for an SNMP server community, the switch applies the default value (read-only). Stations with read-only access can only retrieve MIB objects and stations with read-write access can retrieve, and modify MIB objects.

Clearing SNMP server community read or write access

Use this procedure to clear the SNMP server community read or write access configuration.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
no snmp-server community {ro|rw|<community-string>}
```

Variable definitions

The following table describes the parameters for the **no snmp-server community** command.

Variable	Value
ro | rw	Clears the SNMP server community read—only or write—only access configuration. If you do not specify read-only or read-write, all community strings are removed. If you specify read-only or read-write, just the read-only or read-write community is removed.
<community-string>	Deletes the specified community string from the SNMPv23 MIBs.

Configuring SNMP server community access views

Use this procedure to create community strings with varying levels of read, write, and notification access based on SNMPv3 views.

Note:

These community strings are separate from those created in *Configuring read or write SNMP server community access*.

Before you begin

- Use this command in the Global Configuration mode.

About this task

This command affects community strings stored in the SNMPv3 community table, which allows several community strings to be created. These community strings can have any MIB view.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server community <WORD> [read-view <view-name> | write-view
   <view-name> | notify-view <view-name> | ro | rw]
   ```

Variable definitions

The following table describes the parameters for the **snmp-server community** command.

Variable	Value
<*WORD*>	Specifies the SNMP community string.
read-view<*view-name*>	Changes the read view used by the new community string for different types of SNMP operations. <*view-name*>—specifies an alphanumeric string that names the view, which is a set of MIB objects or instances that you can access.
write-view<*view-name*>	Changes the write view used by the new community string for different types of SNMP operations. <*view-name*>—specifies an alphanumeric string that names the view, which is a set of MIB objects or instances that you can access.
notify-view<*view-name*>	Changes the notify view settings used by the new community string for different types of SNMP operations. <*view-name*>—specifies an alphanumeric string that names the view, which is a set of MIB objects or instances that you can access.
ro	Specifies read-only access for the community string.
rw	Specifies read-write access for the community string.

Configuring an SNMP server system contact

Use this procedure to add or remove a contact person name for a managed SNMP server system node.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] snmp-server contact <name>
   ```

Variable definitions

The following table describes the parameters for the **snmp-server contact** command.

Variable	Value
default	Restores SNMP server system contact to default.
no	Disables SNMP server system contact.
<name>	Specifies an alphanumeric character string that identifies a contact person for a managed SNMP server system node.

Adding or deleting an SNMP trap receiver

Use this procedure to add SNMP trap receivers to the trap receiver table or remove trap receivers from the table.

About this task

With the proprietary method, the table has a maximum of four entries, and these entries can generate only SNMPv1 traps. This command controls the contents of the s5AgTrpRcvrTable, which is the set of trap destinations controlled by the SNMP Configuration screen in the console interface.

Using the standards-based SNMP method, you can create several entries in SNMPv3 MIBs. Each can generate v1 or v2c, or v3 traps.

Important:

Before using the desired community string or user in this command, ensure that the string or user is configured with a notify-view.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To use the proprietary method, enter the following command:

   ```
   [default] [no] snmp-server host <host-ip> <community-string>
   ```

3. To use the standards-based SNMP method, enter the following command:

   ```
   [default] [no] snmp-server host <host-ip> [port <trap-port>] {v1
   <community-string> | v2c <community-string> | v3 {auth|no-auth|auth-
   priv} <username>}
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server host`** command.

Variable	Value
[default]	Clears the SNMP trap receiver table.
host-ip	Specifies the IP address of a host for the trap destination.
community-string	If you use the proprietary method for SNMP, this parameter specifies a community string that works as a password and permits access to the SNMP protocol.
[no]	Deletes the specified SNMP trap receiver from the trap-receiver table.
port<*trap-port*>	Specifies a value for the SNMP trap port between 1 and 65535.
v1<*community-string*>	To configure the standards-based tables, using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.
v2c<*community-string*>	To configure the new standards-based tables, using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.
v3 *{auth|no-auth|auth-priv}*	To configure the new standards-based tables, using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created. Values include: • auth — specifies SNMPv3 traps are sent using authentication and no privacy. • no-auth — specifies SNMPv3 traps are sent using with no authentication and no privacy. • auth-priv — specifies traps are sent using authentication and privacy; this parameter is available only if the image has full SHA/DES support.
username	Specifies an alphanumeric SNMPv3 username for trap destination, when you configure the standards-based table.

Displaying SNMP trap destination information

Use this procedure to display the current SNMP host trap destination information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show snmp-server host
   ```

Enabling or disabling SNMP trap notifications

Use this procedure to enable or disable SNMP trap notifications by notification type.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] snmp-server notification-control <WORD/1-128>
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server notification-control`** command.

Variable	Value
[default]	Restores the specified SNMP trap notification to the default value (Disabled).
[no]	Disables the specified SNMP trap notification.
<WORD/1-128>	Specifies an alphanumeric description or the OID of a supported notification type.

Enabling or disabling SNMP trap notification control for ports

Use this procedure to enable or disable SNMP traps for specific ports, or for all switch ports. You can also use this procedure to reset the SNMP traps to the default value (disabled) for specific ports, or for all switch ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] [default] snmp-server notification-control <WORD> <portlist>
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server notification-control`** command.

Variable	Value
[no]	Disables SNMP traps for specific ports, or for all switch ports
[default]	Sets SNMP traps to the default value (disabled).
<WORD>	Specifies a character string or OID describing the notification type. An example of a character string describing the notification type is `linkDown, linkup`. An example of an OID describing the notification type is `1.3.6.1.6.3.1.1.5.3, 1.3.6.1.6.3.1.1.5.4`.
<portlist.	Specifies a port or group of ports. If you do not specify a port or group of ports, the notification control is disabled for all switch ports.

Viewing SNMP trap notifications

Use this procedure to display a list of SNMP trap notification types and the status of each type.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show snmp-server notification-control
```

Configuring port link status SNMP trap generation

Use this procedure to enable or disable the generation of *linkUp* or *linkDown* SNMP traps for one or more switch ports.

Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. To enable port link status trap generation, enter either of the following commands:

```
snmp trap link-status [port] enable
```

OR

```
default snmp trap link-status [port]
```

3. To disable port link status trap generation, enter either of the following commands:

```
snmp trap link-status [port] disable
```

OR

```
no snmp trap link-status [port]
```

Variable definitions

The following table describes the parameters for the **`snmp trap link-status`** and **`no snmp trap link-status`** commands.

Variable	Value
[port]	Specifies a port or list of ports other than the port or ports you accessed with the **`interface Ethernet`** command.

Configuring the SNMP system location value

Use this procedure to configure the SNMP system location value.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] snmp-server location <location_value>
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server location`** command.

Variable	Value
[default]	Restores the SNMP system location value to default.
[no]	Clears the SNMP system location value.
<location_value>	Specifies an alphanumeric value, with a maximum of 255 characters, for the SNMP system location.

Configuring the SNMP system name

Use this procedure to configure a value for the SNMP system name.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] snmp-server name <name_value>
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server name`** command.

Variable	Value
[default]	Restores the the SNMP system name to default.
[no]	Clears the SNMP system name.
<name_value>	Specifies an alphanumeric value, with a maximum of 255 characters, for the SNMP system name.

Creating an SNMPv3 user with unauthenticated access

Use this procedure to create an SNMPv3 user with unauthenticated read, write, or notify access views.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server user <username> [engine-id <engine-id>] [read-view
   <view-name>] [write-view <view-name>] [notify-view <view-name>]
   ```

Variable definitions

The following table describes the parameters for the **`snmp-server user`** command, when used to create an SNMPv3 user with unauthenticated access.

Variable	Value
<username>	Specifies an alphanumeric user name, with a maximum of 255 characters.
engine-id *<engine-id>*	Specifies the SNMP engine ID for the remote user.
read-view*<view-name>*	Specifies the read view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
write-view*<view-name>*	Specifies the write view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
notify-view*<view-name>*	Specifies the notify view to which the new user has access.

Variable	Value
	view-name—is an alphanumeric value with a maximum of 255 characters.

Important:

If you omit a view parameter from the command, that view type cannot be accessed.

Creating an SNMPv3 user with authenticated access

Use this procedure to create an SNMPv3 user with authenticated read, write, or notify access views.

Note:

If you do not specify view parameters for authenticated access, the user will have access to the views specified for unauthenticated access.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server user <username> [engine-id <engine-id>] md5|sha
   <password> [read-view <view-name>] [write-view <view-name>] [notify-
   view <view-name>]
   ```

   Important:

   You must specify the md5 or sha parameter.

Variable definitions

The following table describes the parameters for the **`snmp-server user`** command, when used to create an SNMPv3 user with authenticated access.

Variable	Value
<username>	Specifies an alphanumeric user name, with a maximum of 255 characters.
engine-id *<engine-id>*	Specifies the SNMP engine ID for the remote user.
md5|sha*<password>*	Specifies the use of an md5 or sha password. *password* — Specifies the new user password; enter an alphanumeric string. If this parameter is omitted,

Variable	Value
	the user is created with only unauthenticated access rights.
read-view<*view-name*>	Specifies the read view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
write-view<*view-name*>	Specifies the write view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
notify-view<*view-name*>	Specifies the notify view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.

Important:

If you omit a view parameter from the command, that view type cannot be accessed.

Creating an SNMPv3 user with authenticated and encrypted access

Use this procedure to create an SNMPv3 user with authenticated and encrypted read, write, or notify access views.

Note:

If you do not specify view parameters for encrypted access, the user has access to the views specified for authenticated access or, if no authenticated views are specified, the user has access to the views specified for unauthenticated access.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server user <username> | engine-id <engine-id> [read-view
   <view-name>] [write-view view-name>] [notify-view <view-name>] md5|
   sha <password> [read-view <view-name>] [write-view <view-name>]
   ```

```
[notify-view <view-name>] 3des|aes|des <password> [read-view <view-
name>] [write-view <view-name>] [notify-view <view-name>]
```

Important:

You must specify the 3des, aes, or des parameter.

Variable definitions

The following table describes the parameters for the **`snmp-server user`** command, when used to create an SNMPv3 user with authenticated, and encrypted access.

Variable	Value
<username>	Specifies an alphanumeric user name, with a maximum of 255 characters.
engine-id *<engine-id>*	Specifies the SNMP engine ID for the remote user.
md5|sha*<password>*	Specifies the use of an md5 or sha password. *<password>*— Specifies the new user password; enter an alphanumeric string. If this parameter is omitted, the user is created with only unauthenticated access rights.
read-view*<view-name>*	Specifies the read view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
write-view*<view-name>*	Specifies the write view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
notify-view*<view-name>*	Specifies the notify view to which the new user has access. *view-name*—is an alphanumeric value with a maximum of 255 characters.
3des|aes|des *<password>*	Specifies the type of privacy encryption. • 3des — Specifies 3DES privacy protocol • aes — Specifies AES privacy protocol • des — Specifies DES privacy protocol *<password>*— Specifies the encryption password; enter an alphanumeric string.

Important:

If you omit a view parameter from the command, that view type cannot be accessed.

Deleting an SNMPv3 user

Use this procedure to delete a specified SNMPv3 user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no snmp-server user [engine-id <engine-id>] <username>
   ```

   Important:

   If you do not specify any parameters, this command deletes all snmpv3 users from the SNMPv3 tables.

Variable definitions

The following table describes the parameters for the **`no snmp-server user`** command.

Variable	Value
engine-id *<engine-id>*	Specifies the SNMP engine ID for the remote user.
<username>	Specifies an alphanumeric user name, with a maximum of 255 characters.

Creating an SNMPv3 view

Use this procedure to create an SNMPv3 view.

About this task

An SNMPv3 view is a set of MIB object instances which can be accessed.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   snmp-server view <view_name> <OID> [<OID> | <OID> | <OID> | <OID> |
   <OID> | <OID> | <OID> | <OID> | <OID>]
   ```

Variable definitions

The following table describes the parameters for the **snmp-server view** command.

Variable	Value
<view_name>	Specifies an alphanumeric value that provides a unique name for the SNMPv3 view.
<OID>	Specifies Object identifier. OID can be entered as a dotted form OID. Each OID must be preceded by a + or - sign (if this is omitted, a + sign is implied). The + is not optional. For the dotted form, a sub-identifier can be an asterisk, indicating a wildcard. The following are examples of valid OID parameters: • sysName • +sysName • -sysName • +sysName.0 • +ifIndex.1 • -ifEntry..1 (this matches all objects in the ifTable with an instance of 1; that is, the entry for interface #1) • 1.3.6.1.2.1.1.1.0 (the dotted form of sysDescr) The + or - indicates whether the specified OID is included in or excluded from, the set of MIB objects accessible using this view. There are 10 possible OID values.

Deleting an SNMPv3 view

Use this procedure to delete a specified SNMPv3 view.

About this task

An SNMPv3 view is a set of MIB object instances which can be accessed.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
no snmp-server view <view_name>
```

Variable definitions

The following table describes the parameters for the **no snmp-server view** command.

Variable	Value
<view_name>	Specifies an alphanumeric value that provides a unique name for the SNMPv3 view.

Securing SNMPv3 communications

Use this procedure to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards.

About this task

The **snmp-server bootstrap** command creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). This commands creates a set of initial users, groups and views.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
snmp-server bootstrap <minimum-secure>| <semi-secure> | <very-secure>
```

Important:

This command deletes all existing SNMP configurations.

Variable definitions

The following table describes the parameters for the **snmp-server bootstrap** command.

Variable	Value
<minimum-secure>	Specifies a minimum security configuration that allows read access and notify access to all processes (view restricted) with noAuth-noPriv and read, write, and notify access to all processes (internet view) using Auth-noPriv and Auth-Priv. **Important:** In this configuration, view restricted matches view internet.
<semi-secure>	Specifies a minimum security configuration that allows read access and notify access to all processes (view restricted) with noAuth-noPriv and read, write, and notify access to all processes (internet view) using Auth-noPriv and Auth-Priv. **Important:** In this configuration, restricted contains a smaller subset of views than internet view.
<very-secure>	Specifies a maximum security configuration that allows no access to the users.

Chapter 7: SNMP configuration using EDM

You can use the information in this chapter to monitor devices running software that supports the retrieval of SNMP information, using Enterprise Device Manager (EDM).

Related Links

Displaying the SNMP configuration on page 157
SNMP MIB view management on page 158
SNMP user management on page 160
Displaying detailed SNMP user information on page 163
SNMP community management on page 164
Displaying detailed SNMP community information on page 166
SNMP host management on page 167
Selecting SNMP host trap notifications on page 171
Configuring SNMP trap notification control on page 179

Displaying the SNMP configuration

Use this procedure to display SNMP configuration information for the switch.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the Chassis work area, click the **SNMP** tab.

Variable definitions

Variable	Value
LastUnauthenticatedInetAddressType	Indicates the last IP address type that was not authenticated by the switch.
LastUnauthenticatedInetAddress	Indicates the last IP address that was not authenticated by the switch.

Variable	Value
LastUnauthenticatedCommunityString	Indicates the last community string that was not authenticated by the switch.
RemoteLoginInetAddressType	Indicates the type of IP address to last remotely log on to the system.
RemoteLoginInetAddress	Indicates the last IP address to remotely log on to the system.
TrpRcvrMaxEnt	Indicates the maximum number of trap receiver entries.
TrpRcvrCurEnt	Indicates the current number of trap receiver entries.
TrpRcvrNext	Indicates the next trap receiver entry to be created.

SNMP MIB view management

You can use the information in this section to display, create, and delete SNMP MIB views.

Displaying SNMP MIB views

Use this procedure to information about existing SNMP MIB views.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Snmp Server**.
3. In the Snmp Server tree, click **MIB View**.

Variable definitions

Variable	Value
ViewName	Indicates the name of the family of view subtrees.
Subtree	Indicates the MIB subtree.
Type	Indicates whether the subtree is included or excluded from the MIB view.
Storage Type	Indicates the memory type in which the table entry is stored. Values include: • **volatile**: The MIB table entry is deleted if the switch loses power. • **nonVolatile**: The MIB table entry is retained if the switch loses power.

Variable	Value
	• **readOnly**: The MIB table entry cannot be changed or deleted.

Creating an SNMP MIB view

Use this procedure to create a new SNMP MIB view.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **MIB View**.
4. On the MIB View work area toolbar, click **Insert**.
5. Configure parameters for the new MIB view as required.
6. Click **Insert**.
7. On the toolbar, you can click **Refresh** to verify the MIB view configuration.

Variable definitions

Variable	Value
ViewName	Specifies an alphanumeric name for the new SNMP MIB view, ranging between 1 and 32 characters.
Subtree	Specifies a valid object identifier that defines the set of MIB objects accessible by this SNMP entity. For example, 1.3.6.1.1.5
Type	Determines whether access to a MIB object is granted (*included*) or denied (*excluded*). DEFAULT: included
StorageType	Specifies the type of memory in which to store the MIB view. Values include: • **volatile**: The MIB entry is deleted if the switch loses power. • **nonVolatile**: The MIB entry is retained if the switch loses power.

Deleting an SNMP MIB view

Use this procedure to delete an existing SNMP MIB view.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **MIB View**.
4. In the MIB View work area, click the row of the MIB view to delete.
5. On the toolbar, click **Delete**.
6. In the confirmation window, click **Yes**.
7. On the toolbar, you can click **Refresh** to verify that the MIB view is deleted.

SNMP user management

You can use the information in this section to create, delete, or display basic information about an SNMP user.

Displaying basic SNMP user information

Use this procedure to display basic switch SNMP user configuration information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **User**.

Variable definitions

Variable	Value
EngineID	Indicates the administratively-unique identifier of the SNMP engine for the user.
Name	Indicates the alphanumeric name assigned to the user.
Auth Protocol	Indicates the registration point for standards-track authentication protocols used in the SNMP management framework.
Priv Protocol	Indicates the privacy protocol assigned to the user.
Storage Type	Indicates the type of memory in which the user configuration is stored. Values include: • **volatile**: The user configuration is lost if the switch loses power.

Variable	Value
	• **nonVolatile**: The user configuration is retained if the switch loses power.

Creating an SNMP user

Use this procedure to create a new SNMP user.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **User**.
4. On the User work area toolbar, click **Insert**.
5. In the Insert User window, configure parameters for the new SNMP user as required.
6. Click **Insert**.
7. On the toolbar, you can click **Refresh** to verify the SNMP user configuration.

Variable definitions

Variable	Value
Name	Specifies an alphanumeric name, ranging between 1 and 32 characters, to assign to the new user.
Auth Protocol	Specifies an authentication protocol for the new user. Values include: • **none** • **MD5** • **SHA** DEFAULT: None If you select an authentication protocol, you must enter and confirm an authentication password, and select a privacy protocol.
AuthPassword	Specifies a new user authentication password. This field is available only if you select an authentication protocol.
ConfirmPassword	Confirms new user authentication password. This field is available only if you select an authentication protocol.

Variable	Value
Priv Protocol	Specifies the new user privacy protocol. Values include: • **none** • **DES** • **3DES** • **AES** If you select a privacy protocol, you must enter and confirm an privacy password. This field is available only if you select a new user authentication protocol.
PrivacyPassword	Specifies a new user privacy password. This field is available only if you select a new user privacy protocol.
ConfirmPassword	Confirms new user privacy password. This field is available only if you select a new user privacy protocol.
ReadViewName	Specifies the SNMP context read access, MIB view name for the new user.
WriteViewName	Specifies the SNMP context write access, MIB view name for the new user.
NotifyViewName	Specifies the SNMP context notification access, MIB view name for the new user.
StorageType	Specifies the type of memory in which to store the new user configuration. Values include: • **volatile**: The user configuration is deleted if the switch loses power. • **nonVolatile**: The user configuration is retained if the switch loses power.

Deleting an SNMP user

Use this procedure to delete an existing SNMP user.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **User**.
4. In the User work area, click the row of the user to delete.

5. On the toolbar, click **Delete**.
6. In the confirmation window, click **Yes**.
7. On the toolbar, you can click **Refresh** to verify that the user is deleted.

Displaying detailed SNMP user information

Use this procedure to display detailed switch SNMP user configuration information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **User**.
4. In the User work area, click a user row.
5. On the toolbar, click **Details**.

Variable definitions

Variable	Value
Name	Indicates the alphanumeric name assigned to the user.
ContextPrefix	Indicates the SNMP context prefix for the user.
SecurityModel	Indicates the security model for the user.
SecurityLevel	Indicates the minimum security level for the user.
ReadViewName	Indicates the SNMP context read access, MIB view name for the user.
WriteViewName	Indicates the SNMP context write access, MIB view name for the user.
NotifyViewName	Indicates the SNMP context notification access, MIB view name for the user.
Storage Type	Indicates the type of memory in which the user configuration is stored. Values include: • **volatile**: The user configuration is lost if the switch loses power. • **nonVolatile**: The user configuration is retained if the switch loses power.

SNMP community management

You can use the information in this section to manage community strings that SNMP-based applications can use to gain access to switch management information.

Displaying basic SNMP community information

Use this procedure to display basic information about configured community strings that SNMP-based applications can use to gain access to switch management information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.

Variable definitions

Variable	Value
Index	Indicates the alphanumeric index identifier for the community string, ranging between 1 and 32 characters.
Name	Indicates that a secret alphanumeric name, ranging between 1 and 32 characters, is assigned to the community string. **Note:** The specific alphanumeric characters of the secret community string name are represented by asterisks (*).
ContextEngineID	Indicates the administratively-unique context identifier of the SNMP engine for the community string.
Storage Type	Indicates the type of memory in which the community string is stored. Values include: • **volatile**: The community string is deleted if the switch loses power. • **nonVolatile**: The community string is retained if the switch loses power.

Creating an SNMP community

Use this procedure to create a new community string that SNMP-based applications can use to gain access to switch management information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.
4. On the Community work area toolbar, click **Insert**.
5. In the Insert Community window, configure parameters for the new SNMP community string as required.
6. Click **Insert**.
7. On the toolbar, you can click **Refresh** to verify the SNMP community string configuration.

Variable definitions

Variable	Value
Index	Specifies an alphanumeric index identifier for the new community string, ranging between 1 and 32 characters.
CommunityName	Specifies a secret alphanumeric name for the new community string, ranging between 1 and 32 characters.
ConfirmCommunity	Confirms the secret name for the new community string.
ReadViewName	Specifies the SNMP context read access, MIB view name for the new community string.
WriteViewName	Specifies the SNMP context write access, MIB view name for the new community string.
NotifyViewName	Specifies the SNMP context notification access, MIB view name for the new community string.
StorageType	Specifies the type of memory in which to store the new community string. Values include: • **volatile**: The community string is deleted if the switch loses power. • **nonVolatile**: The community string is retained if the switch loses power.

Deleting an SNMP community

Use this procedure to delete an existing SNMP community string that SNMP-based applications used to gain access to switch management information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.
4. In the Community work area, click the row of the community string to delete.
5. On the toolbar, click **Delete**.
6. In the confirmation window, click **Yes**.
7. On the toolbar, you can click **Refresh** to verify that the community string is deleted.

Displaying detailed SNMP community information

Use this procedure to display detailed information about configured community strings that SNMP-based applications can use to gain access to switch management information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.
4. In the Community work area, click a community row.
5. On the toolbar, click **Details**.

Variable definitions

Variable	Value
Name	Indicates that a secret alphanumeric name, ranging between 1 and 32 characters, is assigned to the community string.

Variable	Value
	Note: The specific alphanumeric characters of the secret community string name are represented by asterisks (*).
ContextPrefix	Indicates the SNMP context prefix for the community string.
SecurityModel	Indicates the security model for the community string.
SecurityLevel	Indicates the minimum security level for the community string.
ReadViewName	Indicates the SNMP context read access, MIB view name for the community string.
WriteViewName	Indicates the SNMP context write access, MIB view name for the community string.
NotifyViewName	Indicates the SNMP context notification access, MIB view name for the community string.
Storage Type	Indicates the type of memory in which the community string is stored. Values include: • **volatile**: The community string is deleted if the switch loses power. • **nonVolatile**: The community string is retained if the switch loses power.

SNMP host management

You can use the information in this section to create, delete, and display information about SNMP hosts.

Displaying SNMP host information

Use this procedure to display information about SNMP hosts configured on the switch.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Host**.

Variable definitions

Variable	Value
Domain	Indicates the domain IP address type. Values include: • **IPv4** • **IPv6** DEFAULT: IPv4
DestinationAddress (Port)	Indicates the destination IP address and port. Port values range from 0 to 65535. DEFAULT PORT: 162
Timeout	Indicates the maximum time interval that an application waits for a response. DEFAULT: 1500
RetryCount	Indicates the number of generated message retry attempts the switch makes when a response is not received. Values ranges from 0 to 255. DEFAULT: 3
Type	Indicates the host type. Values include: • **trap** • **inform** DEFAULT: trap
Version	Indicates the SNMP version used for the host. Values include: • **SNMPv1** • **SNMPv2c** • **SNMPv3/USM**
SecurityLevel	Indicates the minimum security level required to gain access rights.
Community / User Name	Indicates that a secret alphanumeric name is assigned to the community string associated with the SNMP host. **Note:** The specific alphanumeric characters of the secret community string name are represented by asterisks (*).

Variable	Value
StorageType	Indicates the type of memory in which the host configuration is stored. Values include: • **volatile**: The host configuration is deleted if the switch loses power. • **nonVolatile**: The host configuration is retained if the switch loses power.

Creating an SNMP host

Use this procedure to create and configure a new SNMP host.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Host**.
4. On the Host work area toolbar, click **Insert**.
5. In the Insert Host window, configure the new SNMP host as required.
6. Click **Insert**.
7. On the Host work area toolbar, you can click **Refresh** to verify the new SNMP host configuration.

Variable definitions

Variable	Value
Domain	Specifies the domain IP address type. Values include: • **IPv4** • **IPv6** DEFAULT: IPv4
DestinationAddress	Specifies the destination IP address.
Port	Specifies the destination port. Values range from 0 to 65535. DEFAULT: 162
Timeout	Specifies the maximum time interval (in 1/100 seconds) that an application waits for a response. Values range from 0 to 2147483647. DEFAULT: 1500

Variable	Value
RetryCount	Specifies the number of generated message retry attempts the switch makes when a response is not received. Values ranges from 0 to 255. DEFAULT: 3
Type	Specifies the host type. Values include: • **trap** • **inform** DEFAULT: trap
Version	Specifies the SNMP version to use for the host. Values include: • **SNMPv1** • **SNMPv2c** • **SNMPv3/USM**
SecurityName	Specifies the secret SNMP community string name to associate with the host as a security name.
SecurityLevel	Specifies the minimum security level required to gain access rights. Values include: • **noAuthPriv** • **authNoPriv** • **authPriv** DEFAULT: noAuthPriv
StorageType	Indicates the type of memory in which to store the host configuration. Values include: • **volatile**: The host configuration is deleted if the switch loses power. • **nonVolatile**: The host configuration is retained if the switch loses power

Deleting an SNMP host

Use this procedure to delete an existing SNMP host.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Host**.
4. In the Host work area, click an SNMP host row.

5. On the toolbar, click **Delete**.
6. In the confirmation window, click **Yes**.
7. On the Host work area toolbar, you can click **Refresh** to verify that the SNMP host is deleted.

Selecting SNMP host trap notifications

Use this procedure to select the trap notifications that an SNMP host transmits.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Host**.
4. In the Host work area, click an SNMP host row.
5. On the Host work area toolbar, click **Notification**.
6. In the Host Notification Controls work area, you can enable (select check box) or disable (clear check box) specific SNMP host notifications as required.
7. In the Host Notification Controls work area toolbar, you can click **Enable All** to enable all SNMP host trap notifications simultaneously.
8. In the Host Notification Controls work area toolbar, you can click **Disable All** to disable all SNMP host trap notifications simultaneously.
9. On the toolbar, click **Apply**.
10. On the toolbar, you can click **Refresh** to verify the SNMP host notification configuration.

Variable definitions

Variable	Value
coldStart(.1.3.6.1.6.3.1.1.5.1)	Enables or disables the SNMP trap notification sent when the system is powered on.
warmStart(.1.3.6.1.6.3.1.1.5.2)	Enables or disables the SNMP trap notification sent when the system restarts due to a management reset.
linkDown(.1.3.6.1.6.3.1.1.5.3)	Enables or disables the SNMP trap notification sent when a port link state changes to down.
linkUp(.1.3.6.1.6.3.1.1.5.4)	Enables or disables the SNMP trap notification sent when a port link state changes to up.

Variable	Value
authenticationFailure(.1.3.6.1.6.3.1.1.5.5)	Enables or disables the SNMP trap notification sent when an authentication failure occurs.
s5EtrSbsMacTableFull(.1.3.6.1.4.1.45.1.6.2.1.0.1)	Enables or disables the SNMP trap notification sent when the MAC security address table is full.
s5EtrSbsMacTableClearedForPort(. 1.3.6.1.4.1.45.1.6.2.1.0.2)	Enables or disables the SNMP trap notification sent when the MAC security address table is cleared for a specific port.
s5EtrSbsMacTableCleared(. 1.3.6.1.4.1.45.1.6.2.1.0.3)	Enables or disables the SNMP trap notification sent when the MAC security address table is cleared for all ports.
s5EtrSbsMacRemoved(.1.3.6.1.4.1.45.1.6.2.1.0.4)	Enables or disables the SNMP trap notification sent when a MAC address is removed from the MAC security address table.
s5EtrNewSbsMacAccessViolation(. 1.3.6.1.4.1.45.1.6.2.1.0.5)	Enables or disables the SNMP trap notification sent when the switch detects a MAC address based security violation on a port.
s5EtrMacAddressTablesThresholdReached(. 1.3.6.1.4.1.45.1.6.2.1.0.12)	Enables or disables the SNMP trap notification sent when the threshold of the MAC address table is reached, to avoid an overflow.
s5CtrNewHotSwap(.1.3.6.1.4.1.45.1.6.2.4.0.1)	Enables or disables the SNMP trap notification sent when a component or sub component is inserted or removed from the switch chassis.
s5CtrNewProblem(.1.3.6.1.4.1.45.1.6.2.4.0.2)	Enables or disables the SNMP trap notification sent when a component or sub component experiences a problem warning (nonfatal, or fatal).
s5CtrNewUnitUp(.1.3.6.1.4.1.45.1.6.2.4.0.3)	Enables or disables the SNMP trap notification sent when a new component or sub component is detected.
s5CtrNewUnitDown(.1.3.6.1.4.1.45.1.6.2.4.0.4)	Enables or disables the SNMP trap notification sent when a component or sub component is no longer detected.
s5CtrFanDirectionError(.1.3.6.1.4.1.45.1.6.2.4.0.6)	Enables or disables the SNMP trap notification sent when a cooling fan direction error is detected.
s5CtrHighTemperatureError(. 1.3.6.1.4.1.45.1.6.2.4.0.7)	Enables or disables the SNMP trap notification sent when the system overheats.
bsveVrrpTrapStateTransition(. 1.3.6.1.4.1.45.5.11.0.1)	Enables or disables the SNMP trap notification sent when a state transition occurs on a specific VRRP interface.
bsDhcpSnoopingBindingTableFull(. 1.3.6.1.4.1.45.5.17.0.1)	Enables or disables the SNMP trap notification sent when an attempt is made to add a new DHCP binding entry when the binding table is full.
bsDhcpSnoopingTrap(.1.3.6.1.4.1.45.5.17.0.2)	Enables or disables the SNMP trap notification sent when a DHCP packet is dropped.

Variable	Value
bsDhcpOption82MaxLengthExceeded(. 1.3.6.1.4.1.45.5.17.0.3)	Enables or disables the SNMP trap notification sent when the DHCP Option 82 information could not be added to a DHCP packet because the resulting packet would be too long.
bsDhcpSnoopingExtSaveEntryMACConflict(. 1.3.6.1.4.1.45.5.17.0.4)	Enables or disables the SNMP trap notification sent when a DHCP snooping binding entry is not restored from an external file due to a MAC conflict.
bsDhcpSnoopingExtSaveEntryInvalidInterface(. 1.3.6.1.4.1.45.5.17.0.5)	Enables or disables the SNMP trap notification sent when a DHCP snooping binding entry is not restored from an external file due to a non-existing interface.
bsDhcpSnoopingExtSaveEntryLeaseExpired(. 1.3.6.1.4.1.45.5.17.0.6)	Enables or disables the SNMP trap notification sent when a DHCP snooping binding entry is not restored from an external file because the client lease expired.
bsDhcpSnoopingExtSaveEntryParsingFailure(. 1.3.6.1.4.1.45.5.17.0.7)	Enables or disables the SNMP trap notification sent when a DHCP snooping binding entry is not restored from an external file due to a parsing failure.
bsDhcpSnoopingExtSaveNTP(. 1.3.6.1.4.1.45.5.17.0.8)	Enables or disables the SNMP trap notification sent when the DHCP snooping external save feature is enabled without synchronizing the switch to an NTP server.
bsDhcpSnoopingExtSaveUSBSyncSuccess(. 1.3.6.1.4.1.45.5.17.0.9)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table is successfully saved to a USB drive external file.
bsDhcpSnoopingExtSaveTFTPSyncSuccess(. 1.3.6.1.4.1.45.5.17.0.10)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table is successfully saved to a TFTP server external file.
bsDhcpSnoopingExtSaveUSBSyncFailure(. 1.3.6.1.4.1.45.5.17.0.11)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table cannot save to a USB drive external file.
bsDhcpSnoopingExtSaveTFTPSyncFailure(. 1.3.6.1.4.1.45.5.17.0.12)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table cannot save to a TFTP server external file.
bsDhcpSnoopingExtSaveUSBRestoreSuccess(. 1.3.6.1.4.1.45.5.17.0.13)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table is successfully restored from a USB drive external file.
bsDhcpSnoopingExtSaveTFTPRestoreSuccess(. 1.3.6.1.4.1.45.5.17.0.14)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table is successfully restored from a TFTP server external file.
bsDhcpSnoopingExtSaveUSBRestoreFailure(. 1.3.6.1.4.1.45.5.17.0.15)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table cannot restore from a USB drive external file.

Variable	Value
bsDhcpSnoopingExtSaveTFTPRestoreFailure(. 1.3.6.1.4.1.45.5.17.0.16)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table cannot restore from a TFTP server external file.
bsDhcpSnoopingExtSaveEntryInvalidVlan(. 1.3.6.1.4.1.45.5.17.0.17)	Enables or disables the SNMP trap notification sent when the DHCP snooping binding table is not restored from an external file due to an invalid Vlan ID.
bsDhcpSnoopingExtSaveEntryIfTrustedConflict(. 1.3.6.1.4.1.45.5.17.0.22)	Enables or disables the SNMP trap notification sent when a DHCP snooping binding entry is not restored from an external file on a trusted interface.
bsDhcpSnoopingNotifications.23(. 1.3.6.1.4.1.45.5.17.0.23)	Enables or disables the SNMP trap notification sent when a DHCP packet is dropped because a static entry with the same MAC address was found in the binding table.
bsaiArpPacketDroppedOnUntrustedPort(. 1.3.6.1.4.1.45.5.18.0.1)	Enables or disables the SNMP trap notification sent when an ARP packet is dropped on an untrusted port due to invalid IP/MAC binding.
bsSourceGuardReachedMaxIpEntries(. 1.3.6.1.4.1.45.5.20.0.1)	Enables or disables the SNMP trap notification sent when the maximum IP entries on the port has been reached.
bsSourceGuardCannotEnablePort(. 1.3.6.1.4.1.45.5.20.0.2)	Enables or disables the SNMP trap notification sent when insufficient resources are available to enable IPSG on the port.
bsUnicastStormControlBelowLowWatermark(. 1.3.6.1.4.1.45.5.22.0.1)	Enables or disables the SNMP trap notification sent when the unicast storm control packet rate falls below the low watermark after having risen above the high watermark.
bsUnicastStormControlAboveHighWatermark(. 1.3.6.1.4.1.45.5.22.0.2)	Enables or disables the SNMP trap notification sent when the unicast storm control packet rate remains above the higher watermark.
bsDdiSfpTempAlarm(.1.3.6.1.4.1.45.5.29.0.1)	Enables or disables the SNMP trap notification sent when the SFP Temperature reaches the high temperature alarm level.
bsDdiSfpTempWarn(.1.3.6.1.4.1.45.5.29.0.2)	Enables or disables the SNMP trap notification sent when the SFP Temperature reaches the high temperature warning level.
bsDdiSfpTempNormal(.1.3.6.1.4.1.45.5.29.0.3)	Enables or disables the SNMP trap notification sent when the SFP Temperature returns to the normal temperature level.
bsDdiSfpVoltageAlarm(.1.3.6.1.4.1.45.5.29.0.4)	Enables or disables the SNMP trap notification sent when the SFP Voltage reaches the high voltage alarm level.

Variable	Value
bsDdiSfpVoltageWarn(.1.3.6.1.4.1.45.5.29.0.5)	Enables or disables the SNMP trap notification sent when the SFP Voltage reaches the high voltage warning level.
bsDdiSfpVoltageNormal(.1.3.6.1.4.1.45.5.29.0.6)	Enables or disables the SNMP trap notification sent when the SFP Voltage returns to the normal voltage level.
bsDdiSfpBiasAlarm(.1.3.6.1.4.1.45.5.29.0.7)	Enables or disables the SNMP trap notification sent when the SFP TX Bias reaches the alarm level.
bsDdiSfpBiasWarn(.1.3.6.1.4.1.45.5.29.0.8)	Enables or disables the SNMP trap notification sent when SFP TX Bias reaches the warning level.
bsDdiSfpBiasNormal(.1.3.6.1.4.1.45.5.29.0.9)	Enables or disables the SNMP trap notification sent when SFP TX Bias returns to the normal level.
bsDdiSfpTxAlarm(.1.3.6.1.4.1.45.5.29.0.10)	Enables or disables the SNMP trap notification sent when the SFP TX Power reaches the alarm level.
bsDdiSfpTxWarn(.1.3.6.1.4.1.45.5.29.0.11)	Enables or disables the SNMP trap notification sent when the SFP TX Power reaches the warning level.
bsDdiSfpTxNormal(.1.3.6.1.4.1.45.5.29.0.12)	Enables or disables the SNMP trap notification sent when the SFP TX Power returns to the normal level.
bsDdiSfpRxAlarm(.1.3.6.1.4.1.45.5.29.0.13)	Enables or disables the SNMP trap notification sent when the SFP RX Power reaches the alarm level.
bsDdiSfpRxWarn(.1.3.6.1.4.1.45.5.29.0.14)	Enables or disables the SNMP trap notification sent when the SFP RX Power reaches the warning level.
bsDdiSfpRxNormal(.1.3.6.1.4.1.45.5.29.0.15)	Enables or disables the SNMP trap notification sent when the SFP RX Power returns to the normal level.
bsifnInstallationFailure(.1.3.6.1.4.1.45.5.35.0.1)	Enables or disables the SNMP trap notification sent when an installation failure is detected.
bsLstInterfaceStatusChanged(. 1.3.6.1.4.1.45.5.43.0.1)	Enables or disables the SNMP trap notification sent when a physical or logical interface changes its status in a particular link-state tracking group.
bsLstGroupOperStateChanged(. 1.3.6.1.4.1.45.5.43.0.2)	Enables or disables the SNMP trap notification sent when the operational status of a linkstate tracking group changes due to an interface status change.
bsnConfigurationSavedToNvram(. 1.3.6.1.4.1.45.5.2.2.0.1)	Enables or disables the SNMP trap notification sent when a switch saves its configuration to non volatile storage.
bsnStackManagerReconfiguration(. 1.3.6.1.4.1.45.5.2.2.0.4)	Enables or disables the SNMP trap notification sent when a stack manager detects a problem with a link between stack members.
bsnLacTrunkUnavailable(.1.3.6.1.4.1.45.5.2.2.0.5)	Enables or disables the SNMP trap notification sent when an attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk.

Variable	Value
bsnLoginFailure(.1.3.6.1.4.1.45.5.2.2.0.6)	Enables or disables the SNMP trap notification sent when an attempt to log in to the system fails because of an incorrect password.
bsnTrunkPortDisabledToPreventBroadcastStorm(.1.3.6.1.4.1.45.5.2.2.0.8)	Enables or disables the SNMP trap notification sent when an MLT port is disabled because an MLT trunk is disabled.
bsnTrunkPortEnabledToPreventBroadcastStorm(.1.3.6.1.4.1.45.5.2.2.0.10)	Enables or disables the SNMP trap notification sent when an MLT port is enabled because an MLT trunk is disabled.
bsnLacPortDisabledDueToLossOfVLACPDU(.1.3.6.1.4.1.45.5.2.2.0.11)	Enables or disables the SNMP trap notification sent when a port is disabled due to the loss of a VLACP PDU.
bsnLacPortEnabledDueToReceiptOfVLACPDU(.1.3.6.1.4.1.45.5.2.2.0.12)	Enables or disables the SNMP trap notification sent when a port is enabled due to receipt of a VLACP PDU.
bsnStackConfigurationError(.1.3.6.1.4.1.45.5.2.2.0.13)	Enables or disables the SNMP trap notification sent when the expected size of a stack is not equal to the actual size of the stack.
bsnEnteredForcedStackMode(.1.3.6.1.4.1.45.5.2.2.0.16)	Enables or disables the SNMP trap notification sent when a switch has entered forced stack mode.
bsnSystemUp365Days(.1.3.6.1.4.1.45.5.2.2.0.20)	Enables or disables the SNMP trap notification sent when the system has been up for 365 days.
bsnUSBInsertion(.1.3.6.1.4.1.45.5.2.2.0.21)	This notification is triggered when an USB device is inserted. In stack configuration, s5AgSysUsbTargetUnit specifies the unit number. For standalone, s5AgSysUsbTargetUnit is always 0.
bsnUSBRemoval(.1.3.6.1.4.1.45.5.2.2.0.22)	This notification is triggered when an USB device is removed. In stack configuration, s5AgSysUsbTargetUnit specifies the unit number. For standalone, s5AgSysUsbTargetUnit is always 0.
bsnSFPInsertion(.1.3.6.1.4.1.45.5.2.2.0.23)	This notification is triggered when an SFP module is inserted.
bsnSFPRemoval(.1.3.6.1.4.1.45.5.2.2.0.24)	This notification is triggered when an SFP module is removed.
bsnROPasswordExpired(.1.3.6.1.4.1.45.5.2.2.0.25)	Enables or disables the SNMP trap notification sent when the read only password has expired.
bsnRWPasswordExpired(.1.3.6.1.4.1.45.5.2.2.0.26)	Enables or disables the SNMP trap notification sent when the read/write password has expired.
bsnStackProtection(.1.3.6.1.4.1.45.5.2.2.0.27)	Enables or disables the SNMP trap notifications sent when a stack protection event occurs.

Variable	Value
bsnAaaUserAccountNotUsed (. 1.3.6.1.4.1.45.5.2.2.0.29)	Enables or disables the SNMP trap notification sent when a user account has never been used during a time interval.
bsnAaaAlreadyConnected (. 1.3.6.1.4.1.45.5.2.2.0.30)	Enables or disables the SNMP trap notification sent when a user is connected and attempts to connect again.
bsnAaaIncorrectLogOnThresholdExceeded (. 1.3.6.1.4.1.45.5.2.2.0.31)	Enables or disables the SNMP trap notification sent when the threshold for incorrect user-entered information is exceeded.
bsnAaaMaxNoOfSessionsExceeded (. 1.3.6.1.4.1.45.5.2.2.0.32)	Enables or disables the SNMP trap notification sent when the maxim number of current sessions for an AAA user account is exceeded.
lldpRemTablesChange(.1.0.8802.1.1.2.0.0.1)	Enables or disables the SNMP trap notification sent when the value of **lldpStatsRemTableLastChangeTime** changes. This notification can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.
risingAlarm(.1.3.6.1.2.1.16.0.1)	Enables or disables the SNMP trap notification sent when an alarm entry exceeds the rising threshold and generating an event that is configured for sending SNMP traps.
fallingAlarm(.1.3.6.1.2.1.16.0.2)	Enables or disables the SNMP trap notification sent when an alarm entry exceeds the falling threshold .
newRoot(.1.3.6.1.2.1.17.0.1)	Enables or disables the SNMP trap notification sent when the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, for example, upon expiration of the Topology Change Timer, immediately subsequent to its election.
vrrpTrapNewMaster(.1.3.6.1.2.1.68.0.1)	Enables or disables the SNMP trap notification sent when the sending agent has transition to the Master state.
ospfVirtIfStateChange(.1.3.6.1.2.1.14.16.2.1)	Enables or disables the SNMP trap notification sent when the interface state regresses or progresses to a terminal state.
ospfNbrStateChange(.1.3.6.1.2.1.14.16.2.2)	Enables or disables the SNMP trap notification sent when the neighbor state regresses or progresses to a terminal state.
ospfVirtNbrStateChange(.1.3.6.1.2.1.14.16.2.3)	Enables or disables the SNMP trap notification sent when the virtual neighbor state regresses or progresses to a terminal state.
ospfIfConfigError(.1.3.6.1.2.1.14.16.2.4)	Enables or disables the SNMP trap notification sent when a packet is received on a non-virtual interface from a router with configuration parameters that

Variable	Value
	conflict with the configuration parameters of the local router.
ospfVirtIfConfigError(.1.3.6.1.2.1.14.16.2.5)	Enables or disables the SNMP trap notification sent when a packet is received on a virtual interface from a router with configuration parameters that conflict with the configuration parameters of the local router.
ospfIfAuthFailure(.1.3.6.1.2.1.14.16.2.6)	Enables or disables the SNMP trap notification sent when a packet is received on a non-virtual interface from a router with an authentication key or authentication type that conflicts with the authentication key or authentication type of the local router.
ospfVirtIfAuthFailure(.1.3.6.1.2.1.14.16.2.7)	Enables or disables the SNMP trap notification sent when a packet is received on a virtual interface from a router with an authentication key or authentication type that conflicts with the authentication key or authentication type of the local router.
ospfIfStateChange(.1.3.6.1.2.1.14.16.2.16)	Enables or disables the SNMP trap notification sent when the OSPF interface state regresses or progresses to a terminal state.
entConfigChange(.1.3.6.1.2.1.47.2.0.1)	Enables or disables the SNMP trap notification sent when a hardware change is detected. For example, a unit is added or removed from a stack.
lldpXMedTopologyChangeDetected(. 1.0.8802.1.1.2.1.5.4795.0.1)	Enables or disables the SNMP trap notification sent when the local switch senses a change in the topology. The change indicates that a new remote device is attached to a local port, or a remote device is disconnected, or moved from one port to another.
avFcoeRedirEgressIssueDetected(. 1.3.6.1.4.1.45.4.7.3.3)	Enables or disables the SNMP trap notification when an FCoE redirect egress issue occurs.
slaMonitorAgentExceptionDetected(. 1.3.6.1.4.1.45.4.8.0.1)	Enables or disables the SNMP trap notification when an SLA Mon agent exception notification occurs.
rcnSmltIstLinkUp(.1.3.6.1.4.1.2272.1.21.0.17)	Enables or disables the SNMP trap notification when the IST link transitions from down to up.
rcnSmltIstLinkDown(.1.3.6.1.4.1.2272.1.21.0.18)	Enables or disables the SNMP trap notification when the IST link transitions from up to down.
rcnSmltLinkUp(.1.3.6.1.4.1.2272.1.21.0.19)	Enables or disables the SNMP trap notification when SMLT becomes up (SMLT current type transitions from NORM to SMLT).
rcnSmltLinkDown(.1.3.6.1.4.1.2272.1.21.0.20)	Enables or disables the SNMP trap notification when SMLT goes down (SMLT current type transitions from SMLT to NORM).
rcnBpduReceived(.1.3.6.1.4.1.2272.1.21.0.79)	Enables or disables the SNMP trap notification sent when a BPDU is received on a port which has BPDU filtering enabled.

Variable	Value
rcnIsisPlsbMetricMismatchTrap(. 1.3.6.1.4.1.2272.1.21.0.192)	Enables or disables the SNMP trap notification when an LSP with a different value of L1–metric is received.
rcnIsisPlsbDuplicateSysidTrap(. 1.3.6.1.4.1.2272.1.21.0.193)	Enables or disables the SNMP trap notification when a Hello packet with a duplicate system ID is received.
rcnIsisPlsbLsdbUpdateTrap(. 1.3.6.1.4.1.2272.1.21.0.194)	Enables or disables the SNMP trap notification when LSDB information is changed.
rcnIsisPlsbBvidMismatchTrap(. 1.3.6.1.4.1.2272.1.21.0.278)	Enables or disables the SNMP trap notification when a Hello packet with mismatched LSDB-VIDs is received.
rcnIsisPlsbSmltVirtBmacMismatchTrap(. 1.3.6.1.4.1.2272.1.21.0.279)	Enables or disables the SNMP trap notification sent when the Virtual BMAC configured in the switch is different from the virtual BMAC configured in the IST peer.
rcnIsisPlsbSmltPeerBmacMismatchTrap(. 1.3.6.1.4.1.2272.1.21.0.280)	Enables or disables the SNMP trap notification sent when the Peer BMAC configured in the switch is different from the peer BMAC configured in the IST peer.
rcnIsisPlsbAdjStateTrap(. 1.3.6.1.4.1.2272.1.21.0.281)	Enables or disables the SNMP trap notification when the ISIS adjacency state changes.
rcnIsisPlsbDuplicateNnameTrap(. 1.3.6.1.4.1.2272.1.21.0.282)	Enables or disables the SNMP trap notification when an LSP with a duplicate name is received.
rcnIsisPlsbSmltSplitBebMismatchTrap(. 1.3.6.1.4.1.2272.1.21.0.283)	Enables or disables the SNMP trap notification sent when the Smlt Split-Beb configured in the local switch and IST peer are the same.
rcnIsisPlsbMultiLinkAdjTrap(. 1.3.6.1.4.1.2272.1.21.0.284)	Enables or disables the SNMP trap notification when multiple ISIS adjacencies are formed with the same ISIS node.
rcnSlppPortDownEventNew(. 1.3.6.1.4.1.2272.1.64.1.0.2)	Enables or disables the SNMP trap notification when an SLPP port is down.
rcnSlppGuardHoldDownExpired (. 1.3.6.1.4.1.2272.1.64.1.0.4)	Indicates that the SLPP-guard hold-down timer has expired on a port on which SLPP-guard is enabled, and the port has been re-enabled.
rcnSlppGuardPacketReceived (. 1.3.6.1.4.1.2272.1.64.1.0.5)	Indicates an SLPP packet has been received on a port on which SLPP-guard is enabled. The port has been disabled.

Configuring SNMP trap notification control

Use this procedure to configure notification control for SNMP traps.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Notification Control**.
4. In the Notification Control work area, configure SNMP notification control as required.
5. On the Notification Control work area toolbar, you can click **Enable All** to enable notification control for all SNMP traps simultaneously.
6. On the Notification Control work area toolbar, you can click **Disable All** to disable notification control for all SNMP traps simultaneously.
7. On the toolbar, click **Apply**.
8. On the toolbar, you can click **Refresh** to verify the SNMP trap notification configuration.

Variable definitions

Variable	Value
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (oid)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Enables (true) or disables (false) the SNMP trap.
NotifyControlPortListEnabled	Indicates the port list for which the notification is enabled or disabled. Whether or not this field is configurable depends on the SNMP trap object identifier value.

Chapter 8: DHCP snooping configuration using ACLI

This section describes the procedures you can use to configure Dynamic Host Configuration Protocol (DHCP) snooping to provide security to your network by preventing DHCP spoofing.

Related Links

Configuring DHCP Snooping External Save on page 182

Enabling or disabling DHCP snooping globally

Use this procedure to enable or disable DHCP snooping for the switch.

About this task

Before DHCP snooping can function on a VLAN or port, you must enable DHCP snooping globally. If DHCP snooping is disabled globally, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] ip dhcp-snooping enable
   ```

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping enable`** command.

Variable	Value
[default]	Restores DHCP snooping for the switch to the default value. DEFAULT: disable

Variable	Value
[no]	Disables DHCP snooping for the switch.

Configuring DHCP Snooping External Save

You can configure DHCP Snooping to save the binding table to an external location; either a TFTP server or a USB drive.

Before you begin

- Configure DHCP Snooping on your switch

About this task

If you want to save the DHCP Snooping Binding Table externally, use the following procedure.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter

   ```
   ip dhcp-snooping external-save enable <tftp | usb>
   ```

Related Links

DHCP snooping configuration using ACLI on page 181
Variable definitions on page 182

Variable definitions

You can use the information in the following table to help you understand the **`ip dhcp-snooping external-save`** command.

Variable	Value
enable	Enables external saving of the DHCP snooping binding table.
tftp <*A.B.C.D* | *WORD*>	Saves the DHCP snooping binding table on a TFTP server. • A.B.D.C—the IPv4 address of the TFTP server • WORD—the IPV6 address of the TFTP server

Variable	Value
usb *<filename>* *<unit>*	Saves the DHCP snooping binding table on a USB drive. • filename—the name of the DHCP snooping binding table external file • unit—the USB unit number on which to save the DHCP snooping binding table

Related Links

Configuring DHCP Snooping External Save on page 182

Enabling or disabling DHCP snooping Option 82 globally

Use this procedure to enable or disable DHCP snooping Option 82 for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [default] [no] ip dhcp-snooping option82
   ```

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping option82`** command.

Variable	Value
[default]	Restores DHCP Option 82 for the switch to the default value. DEFAULT: disable
[no]	Disables DHCP Option 82 for the switch.

Displaying the global DHCP snooping configuration status

Use this procedure to view the DHCP snooping and DHCP Option 82 configuration status for the switch, and for all configured VLANs.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-snooping
```

Configuring VLAN-based DHCP snooping

Use this procedure to enable or disable DHCP snooping, or to enable or disable DHCP Option 82 for a specific VLAN.

Important:

If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports associated with the VLAN, regardless of whether the port is trusted or untrusted.

You must enable DHCP snooping for each VLAN separately.

Before you begin

- Enable DHCP snooping globally.

  Important:

  If DHCP snooping is disabled globally, you can enable DHCP snooping on a VLAN, but the switch continues to forward DHCP reply packets to all applicable ports associated with the VLAN, regardless of whether the port is trusted or untrusted.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
[default] [no] ip dhcp-snooping vlan <vlanID> [option82]
```

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping vlan`** command.

Variable	Value
[default]	Restores DHCP snooping or DHCP Option 82 for the VLAN to the default value. DEFAULT: disabled

Variable	Value
[no]	Disables DHCP snooping or DHCP Option 82 for the VLAN. If you do not specify a VLAN ID, DHCP snooping is disabled on all VLANs. **Important:** If you do not specify a VLAN identifier when disabling DHCP snooping, the feature is disabled for all VLANs.
<vlanID>	Specifies the VLAN identifier. Values range from 1 to 4094.
option82	Enables DHCP Option 82 for the VLAN.

Displaying VLAN-based DHCP snooping configuration status

Use this procedure to review and confirm the DHCP snooping and DHCP snooping Option 82 configuration status for all VLANs.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-snooping vlan
```

Configuring port-based DHCP snooping

Use this procedure to configure one or more switch ports to filter DHCP replies through DHCP snooping, or to forward DHCP replies automatically.

Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip dhcp-snooping port <portlist> trusted | untrusted
```

Variable definitions

The following table describes the parameters for the **ip dhcp-snooping port** command.

Variable	Value
[default]	Restores DHCP snooping for the selected port or ports to the default value. DEFAULT: untrusted
<portlist>	Specifies a port or group of ports.
trusted	Specifies that the selected port or ports automatically forward DHCP replies.
untrusted	Specifies that the selected port or ports filter DHCP replies through DHCP snooping.

Restoring DHCP snooping to default for all ports

Use this procedure to restore DHCP snooping for all switch ports to the default value, *untrusted*.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port>
   ```

2. At the command prompt, enter the following command:

   ```
   default ip dhcp-snooping port all
   ```

Configuring the DHCP snooping Option 82 subscriber ID for ports

Use this procedure to assign a DHCP snooping Option 82 subscriber ID to, or remove a DHCP snooping Option 82 subscriber ID from one or more switch ports.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   ```

```
configure terminal

interface Ethernet <port>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip dhcp-snooping port <portlist> option82-subscriber-
id [<WORD>]
```

Variable definitions

The following table describes the parameters for the **ip dhcp-snooping port <portlist> option82-subscriber-id** command.

Variable	Value
[default]	Restores the DHCP snooping Option 82 subscriber ID for the selected port or ports to the default value. DEFAULT: no subscriber ID
[no]	Removes the DHCP snooping Option 82 subscriber ID from the selected port or ports.
<portlist>	Specifies an individual port or list of ports.
[<WORD>]	Specifies an alphanumeric character string for the DHCP snooping Option 82 subscriber ID.

Displaying the port-based DHCP snooping configuration

Use this procedure to display the port-based DHCP snooping configuration status for a specific switch port, a list of switch ports, or all switch ports.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip dchp-snooping interface [<interface_type>] [<portlist>]
```

Variable definitions

The following table describes the parameters for the **show ip dchp-snooping interface** command.

Variable	Value
[<interface_type>]	Specifies the type of interface for which to display the port-based DHCP snooping configuration status.
[<portlist>]	Specifies a specific port or list of ports.

Adding static entries to the DHCP snooping binding table

Use this procedure to add entries for devices with static IP addresses to the DHCP binding table.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   ip dhcp-snooping binding <1-4094> <MAC_addr> ip <IP_addr> port
   <portlist> [expiry <1-4294967295>]
   ```

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping binding`** command.

Variable	Value
<1-4094>	Specifies the ID of the VLAN that the DHCP client is a member of.
<MAC_addr>	Specifies the MAC address of the DHCP client.
ip*<IP_addr>*	Specifies the IP address of the DHCP client.
port*<portlist>*	Specifies the switch port that the DHCP client is connected to.
expiry *<1-4294967295>*	Specifies the time, in seconds, before the DHCP client binding expires. Values range from 1 to 4294967295 seconds. DEFAULT: 0

Deleting static entries from the DHCP snooping binding table

Use this procedure to delete entries for devices with static IP addresses from the DHCP binding table, by removing the device MAC address from the table.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no ip dhcp-snooping binding <1-4094> <MAC_addr>
   ```

Variable definitions

The following table describes the parameters for the **`no ip dhcp-snooping binding`** command.

Variable	Value
<1-4094>	Specifies the ID of the VLAN that the DHCP client is a member of.
<MAC_addr>	Specifies the MAC address of the DHCP client.

Displaying the DHCP snooping binding table

Use this procedure to display detailed DHCP snooping binding table entry information.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

   ```
   show ip dhcp-snooping binding
   ```

   Important:

   If you use the **`show ip dhcp-snooping binding`** command on a large stack with a complex configuration, you can experience slow output if this command is executed within 4-5 minutes of the stack being booted or power-cycled. If you wait 5 minutes after the stack is booted or power-cycled before executing this show command, you will observe normal response times.

Chapter 9: DHCP snooping configuration using EDM

This section describes the procedures you can use to configure Dynamic Host Configuration Protocol (DHCP) snooping to provide security to your network by preventing DHCP spoofing.

Related Links

Configuring DHCP snooping globally on page 190
Configuring DHCP Snooping on a VLAN on page 192
Configuring DHCP Snooping port trust on page 193
DHCP binding configuration on page 194

Configuring DHCP snooping globally

Use the following procedure to configure DHCP snooping globally on the switch.

Warning:

You must enable DHCP snooping on Layer 3 VLANs spanning toward DHCP servers in Layer 3 mode. DHCP relay is also required for correct operation.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **DHCP Snooping.**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. To enable DHCP snooping globally, click the **DhcpSnoopingEnabled** box.
5. To enable Option 82 for DHCP snooping, click the **DhcpSnoopingOption82Enabled** box.
6. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
DhcpSnoopingEnabled	Enables or disables DHCP Snooping globally.
DhcpSnoopingOption82Enabled	Enables or disables DHCP Snooping option 82 globally.

Configuring DHCP Snooping external save

Use this procedure to store the DHCP Snooping database to an external TFTP server or USB drive.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. In the **DHCP Snooping External Save** section, select the **Enabled** check box, to enable DHCP Snooping external save. Uncheck this box to disable DHCP Snooping external save.
5. Click a **TftpServerAddressType** button.
6. Type a value in the **TftpServerAddress** box.
7. Type a value in the **UsbTargetUnit** box.
8. Type a value in the **Filename** box.
9. To force a binding table restore, click the **ForceRestore** button.
10. On the toolbar, click **Apply**

Variable definitions

Variable	Value
Enabled	Enables or disables DHCP Snooping External Save.
SyncFlag	Indicates if changes in the DHCP Snooping binding table are synchronized on the external device. Values include: • **true**: changes will be synchronized at the next write operation • **false**: changes will not be synchronized at the next write operation
LastSyncTime	Displays the UTC time when the switch last backed up the DHCP Snooping binding table.

Variable	Value
TftpServerAddressType	Specifies the IP address type of the TFTP server on which to save the DHCP Snooping binding file. Values include ipv4 or ipv6.
TftpServerAddress	Specifies the IPv4 or IPv6 address of the TFTP server on which to save the DHCP Snooping binding file.
UsbTargetUnit	Specifies the unit number of the USB port to use in file save or restore operations.
Filename	Specifies the name of the DHCP Snooping database that is saved externally.
ForceRestore	Forces the restoration of the DHCP Snooping database on the switch from the file previously saved to an external USB drive or TFTP server.

Configuring DHCP Snooping on a VLAN

Use this procedure to enable or disable DHCP snooping on the VLAN.

Important:

You must enable DHCP snooping separately for each Vlan ID.

Important:

If you disable DHCP snooping on a VLAN, the switch forwards DHCP reply packets to all applicable ports, whether the port is trusted or untrusted.

Procedure

1. From the Device Physical View, select a port.
2. From the navigation tree, double-click **Security**.
3. In the Security tree, click **DHCP Snooping**.
4. In the work area, click the **DHCP Snooping-VLAN** tab.
5. To select a VLAN to edit, click the VLAN ID.
6. In the VLAN row, double-click the cell in the **DhcpSnoopingEnabled** column.
7. Select a value from the list**—true**to enable DHCP snooping for the VLAN, or **false** to disable DHCP snooping for the VLAN.
8. In the VLAN row, double-click the cell in the **VlanOtion82Enabled** column.
9. Select a value from the list**—true**to enable DHCP snooping with Option 82 for the VLAN, or **false** to disable DHCP snooping with Option 82 for the VLAN.
10. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
VlanId	Indicates the VlanId on the VLAN.
DhcpSnoopingEnabled	Enables or disables DHCP snooping.
VlanOption82Enabled	Enables or disables DHCP Snooping option 82 for the VLAN.

Configuring DHCP Snooping port trust

Use this procedure to specify whether a particular port or multiple ports are trusted or untrusted. Ports are untrusted by default.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping-port** tab.
4. In the **Make Selection** section, click the **Switch/Stack/Ports** ellipsis.
5. Click a port, a range of ports, or **All**.
6. Click **Ok**.
7. In the **Make Selection** section, double-click in the cell under **DhcpSnoopingIfTrusted**.
8. Click a value in the **DhcpSnoopingIfTrusted** list**—trusted** or **untrusted**.
9. In the **Make Selection** section, double-click in the cell under **DhcpSnoopingIfTrusted**.
10. In the **DhcpSnoopingIfOption82SubscriberId** cell, type a subscriber Id value for the port.
11. Click **Apply Selection**.
12. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
Port	Indicates the port on the switch.
DhcpSnoopingIfTrusted	Indicates whether the port is trusted or untrusted. Default is false.

Variable	Value
DhcpSnoopingIfOption82SubscriberId	Indicates the DHCP option 82 subscriber ID. Value is a character string between 0 and 64 characters..

DHCP binding configuration

Use the information in this section to view and manage DHCP client lease static entries.

Viewing DHCP binding information

Use this procedure to display DHCP binding information.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.

Variable definitions

Variable	Value
VlanId	Indicates the ID of the VLAN that the DHCP client is a member of.
MacAddress	Indicates the MAC address of the DHCP client.
AddressType	Indicates the MAC address type of the DHCP client.
Address	Indicates IP address of the DHCP client.
Interface	Indicates the interface to which the DHCP client is connected.
LeaseTime(sec)	Indicates the lease time (in seconds) of the DHCP client binding. Values range from 0 to 4294967295.
TimeToExpiry(sec)	Indicates the time (in seconds) before a DHCP client binding expires.
Source	Indicates the source of the binding table entry.

Creating static DHCP binding table entries

Use this procedure to add entries for devices with static IP addresses to the DHCP binding table.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.
4. Click **Insert**. The Insert DHCP Bindings dialog box appears.
5. Click the VlanId ellipsis (...).
6. Select the DHCP client VLAN ID.
7. Click **OK** .
8. In the **MacAddress** type the DHCP client MAC address.
9. In the **AddressType** click a button.
10. In the **Address** box, type the DHCP client IP address.
11. Click the Interface ellipsis (...).
12. From the list, click an interface port.
13. Click **OK**.
14. In the **Lease Time(sec)** box, type a lease time.
15. Click **Insert**.
16. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
VlanId	Specifies the ID of the VLAN that the DHCP client is a member of.
MacAddress	Specifies the MAC address of the DHCP client.
AddressType	Specifies the IP address type of the DHCP client.
Address	Specifies IP address of the DHCP client.
Interface	Specifies the interface to which the DHCP client is connected.
LeaseTime(sec)	Specifies the lease time (in seconds) for the DHCP client binding. Values range from 0 to 4294967295. An infinite lease time exists when LeaseTime=0.

Deleting DHCP binding table entries

Use this procedure to delete static IP addresses from the DHCP binding table.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. On the toolbar click **Delete**.
6. Click **Yes** to confirm that you want to delete the entry.

Chapter 10: DAI configuration using ACLI

Enabling or disabling dynamic ARP inspection on a VLAN

Use this procedure to enable or disable the validation of Address Resolution Protocol (ARP) packets on a VLAN.

Dynamic ARP inspection is disabled on VLANs by default.

Note:

You must enable or disable dynamic ARP inspection individually for each VLAN.

Important:

Before you can disable dynamic ARP inspection on a VLAN, you must disable IP Source Guard on port members assigned to the VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] ip arp-inspection vlan <1-4094>
   ```

Variable definitions

The following table describes the parameters for the **`ip arp-inspection vlan`** command.

Variable	Value
[no]	Disables dynamic ARP inspection on the selected VLAN. DEFAULT: Disabled
<1–4094>	Specifies the VLAN identifier (VID). Values range from 1 to 4094.

Configuring dynamic ARP inspection for switch ports

Use this procedure to select whether the dynamic ARP inspection status for one or more switch ports is set to *trusted* or *untrusted*.

The default is untrusted.

About this task

ARP traffic on *trusted* switch ports is not subject to dynamic ARP inspection, while ARP traffic on *untrusted* switch ports is subject to dynamic ARP inspection.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port>
   ```

2. At the command prompt, enter the following command:

   ```
   ip arp-inspection [port <portlist>] trusted | untrusted
   ```

Variable definitions

The following table describes the parameters for the **`ip arp-inspection`** command.

Variable	Value
port<*portlist*>	Specifies a port or list of ports.
trusted	Specifies that ARP traffic on the selected port or ports is not subject to dynamic ARP inspection.
untrusted	Specifies that ARP traffic on the selected port or ports is subject to dynamic ARP inspection.

Restoring dynamic ARP inspection for switch ports to default

Use this procedure to restore the dynamic ARP inspection status for one or more switch ports to default.

About this task

ARP traffic on *trusted* switch ports is not subject to dynamic ARP inspection, while ARP traffic on *untrusted* switch ports is subject to dynamic ARP inspection.

The default is *untrusted*.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port>
   ```

2. At the command prompt, enter the following command:

   ```
   default ip arp-inspection [port <portlist> | all]
   ```

Variable definitions

The following table describes the parameters for the **`default ip arp-inspection`** command.

Variable	Value
port<*portlist*> | *all*	Specifies the port or ports for which to restore the dynamic ARP inspection status to default. • <portlist>—specifies a port or list of ports. • all—specifies all switch ports. DEFAULT: Untrusted

Displaying the dynamic ARP inspection status for switch ports

Use this procedure to display whether dynamic ARP inspection for one or more switch ports is set to *untrusted* or *untrusted*.

About this task

ARP traffic on *trusted* switch ports is not subject to dynamic ARP inspection, while ARP traffic on *untrusted* switch ports is subject to dynamic ARP inspection.

The default is *untrusted*.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show ip arp-inspection interface [<interface_type>] [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the **show ip arp-inspection interface** command.

Variable	Value
<interface_type>	Specifies the type of interface.
<portlist>	Specifies a port or list of ports. If you do not enter a value for this parameter, the dynamic ARP inspection status for all switch ports is displayed.

Displaying the dynamic ARP inspection status for VLANs

Use this procedure to display whether dynamic ARP inspection is enabled or disabled on configured VLANs.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show ip arp-inspection vlan
   ```

Chapter 11: DAI configuration using EDM

Dynamic ARP inspection configuration using EDM

This section describes the procedures you can use to validate ARP packets in a network.

Configuring dynamic ARP inspection on VLANs

Use the following procedure to enable or disable ARP inspection on one or more VLANs.

Procedure

1. From the navigation pane, double-click **Security**.
2. In the Security tree, double-click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-VLAN** tab.
4. In the table, double-click the cell under the column heading **ARPInspectionEnabled** for a VLAN.
5. Select a value (true or false) to enable or disable ARP Inspection-VLAN.
6. Repeat the previous two steps for additional VLANs as required.
7. On the toolbar, click **Apply**.
8. On the toolbar, you can click **Refresh** to verify the ARP Inspection-VLAN configuration.

Variable definitions

Variable	Value
VlanId	Identifies VLANs configured on the switch. RANGE: 1 to 4094
ARPInspectionEnabled	Enables or disables ARP inspection on a VLAN: • **True**: Enables ARP inspection on the specified VLAN(s)

Variable	Value
	• **False**: Disables ARP inspection on the specified VLAN(s). DEFAULT: Disabled

Configuring dynamic ARP inspection on ports

Use this procedure to enable or disable ARP inspection on one or more ports.

Procedure

1. From the navigation pane, double-click **Security**.
2. In the Security tree, click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-port** tab.
4. In the **Make Selection** section, click the **Switch/Stack/Ports** ellipsis.
5. Click a port, a range of ports, or **All**.
6. Click **Ok**.
7. In the **Make Selection** section, double-click in the cell under **ArpInspectionIfTrusted**.
8. Click a value in the **ARPInspectionIfTrusted** list — **trusted** or **untrusted**.
9. Click **Apply Selection**.
10. On the toolbar, click **Apply**.
11. On the toolbar, you can click **Refresh** to verify the ARP inspection on ports configuration.

Variable definitions

Variable	Value
Port	Indicates a port, range of ports, or all ports on the switch.
ArpInspectionIfTrusted	Indicates whether the port is trusted or untrusted. If a port is trusted, ARP traffic is not subject to dynamic ARP inspection. If a port is untrusted, ARP traffic is subject to dynamic ARP inspection. DEFAULT: untrusted

Appendix A: TACACS+ configuration examples

Related Links

TACACS+ configuration example: Avaya Identity Engine Ignition Server on page 203
TACACS+ configuration example: Cisco ACS (version 3.2) server on page 207
TACACS+ configuration example: ClearBox server on page 211
TACACS+ configuration example: Linux freeware server on page 218

TACACS+ configuration example: Avaya Identity Engine Ignition Server

The following section shows the steps required to configure TACACS+ on Avaya Identity Engines Ignition Server, Release 8.0.

A TACACS+ server responds to and audits network access requests. In an Avaya installation, the Identity Engines Ignition Server is the TACACS+ server.

The example displays how to do the following:

- Enable TACACS+
- Configure a user
- Create a command set
- Configure the authentication protocol policy
- Create the authorization policy
- Configure TACACS+ authenticators

For more information on the Avaya Ignition Server, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

Before you begin

- Configure the Ignition Server appliance and set up its network settings. For more information, see *Avaya Identity Engines Ignition Server Getting Started*, NN47280-300.
- Install the Ignition Dashboard on your Windows OS.

- Configure each authenticator (VSP 7000) to recognize the Ignition Server appliance as its TACACS+ server.
- Configure your switch to send packets to the Ignition Server appliance with the appropriate IP address and port.
- Ensure licenses are up-to-date.

Procedure

1. If the Ignition Server Dashboard is not connected to your Ignition Server, select **Administration: Login** to connect.
   a. The default login credentials for **User Name** and **Password** are `admin`/`admin`. Avaya recommends you change the default values.
   b. In the **Connect to** field enter the IP address of the Ignition Server for TACACS+. In this example, the IP address for the TACACS+ server is 192.0.2.8.
2. Enable TACACS+.
   a. In the Ignition Server Dashboard, select **Site 0**.
   b. In the Sites window, select the **Services** tab.
   c. Under the Services tab, select the **TACACS+** tab.
   d. Click the **Edit** button in the TACACS+ tab.
   e. In the Edit TACACS+ Configuration dialog box, select the **Protocol is enabled** box.
   f. In the **Bound Interface** field, select Admin Port.
   g. In the **Port** field, enter `49`.
   h. Select the **Accept Requests from Any Authenticator**.

      Select this option if you want to create a global TACACS+ authenticator that sets policy for all authenticators that do not match a specific TACACS+ enabled authentication in your Ignition server configuration.
   i. In the **Access Policy** field, select **default-tacacs-admin**.

      Use this configuration in the case of a global TACACS+ authenticator. Choose your global TACACS+ policy that you want applied if the device finds no better matching authenticator.
   j. In **TACACS+ Shared Secret** field, enter the secret that the VSP 7000 and TACACS+ Ignition server share. In this example, the shared secret is `secret`.
   k. Click **OK**.
3. Configure a user recognized by the TACACS + server.
   a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration** > **Directories** > **Internal Store** > **Internal Users**.
   b. Click **New**.
   c. Fill in the appropriate fields.

As an example:

User Name: jsmith

First Name: John

Last Name: Smith

Password: test

Confirm password: test

4. If your TACACS+ policy uses per-command authorization, create a command set.
   a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration** > **Access Policies** > **TACACS+**.
   b. Click **Define Command Sets**.
   c. Click **New**.
   d. In the New Device Command Set window, type a **Name** and **Description** for the command set; for instance, level5.

      In this window you build your command set by adding commands to the list. You can build the command list manually or you can import a list. For more information on importing a command list, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
   e. To manually add the commands, click **Add** in the New/Edit Device Command Set window.
   f. Click the **Simple Command Using Keywords and Arguments** box.
   g. In the **Command** field, type the command, and optionally its arguments.
   h. To allow the command to be used with any argument, select the **Allow** box.
   i. To allow only the specific command and arguments you have types, tick the **Deny** box.
   j. Click **OK** to add the command to the list.
   k. Continue to add the commands that you want.
5. If your TACACS+ policy uses privilege-level authorization, create the TACACS+ access policy to allow the TACACS+ Ignition Server to communicate with VSP 7000.
   a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration** > **Access Policies** > **TACACS+**.
   b. Select **default-tacacs-admin**.
   c. Click on the **Authorization Policy** tab and select the name of the policy you want to edit.
   d. Click **Edit** and the **Edit Authorization Policy** window appears.
   e. In the **Rules** section, select the rule you want to edit. In this case select level5, to which you have already added commands.

      The **Rules** list at the left lets you browse and sort the rules in your policy. Use the up and down arrow buttons at the right to set the rule sequence, and click a rule name in

the list to edit that rule. The Selected Rule Details section lets you edit the rule you have selected.

f. In the Selected Rule Details section, under **Rule Name**, for this example, it reads `level5`.

g. Select **Rule Enabled**.

h. With level5 selected in the Rules list, go to the buttons to the right of the **Constraint** list and click **New**.

i. In the Action section, select **Allow**.

j. Select the **Command Sets** tab, in the Action section. Allow Commands in Set should read level-5, in this example, and under All Command Sets all the commands that are accessible under level5 should be listed.

k. Click **OK**.

For this example to function properly, the summary window must display:

IF User: user-id = level5 THEN Allow

Permit commands in Command Set: level-5

6. Configure the Ignition Server to connect to authenticators, which is Avaya Virtual Services Platform 7000:

a. In the Ignition Server Dashboard, expand the following folders: **Site Configuration** > **Authenticators** > **default** and the Authenticator Summary window appears.

b. Click **New**, and the Authenticator Details window appears.

c. For this example, type `VSP7000` under name.

d. To the right select **Enable Authenticator**.

e. Type the IP address for the VSP 7000, which is the authenticator. Use the primary CPU address or the management virtual address.

f. In the **Vendor** field, select **Nortel**.

g. In the **Device template** field, select **ers-switches-nortel**.

h. Select the **TACACS+ Settings** tab.

i. Select **Enable TACACS+ Access**.

j. In the **TACACS+ Shared Secret** field, type the key value you entered into VSP 7000. In this example, the key is the word `secret`.

To connect using TACACS+, you must use the shared secret for each device. In your switch documentation, the shared secret can also be referred to as a specific key string or an encryption string.

k. Under **Access Policy**, select **default-tacacs-user**.

l. Click **OK**.

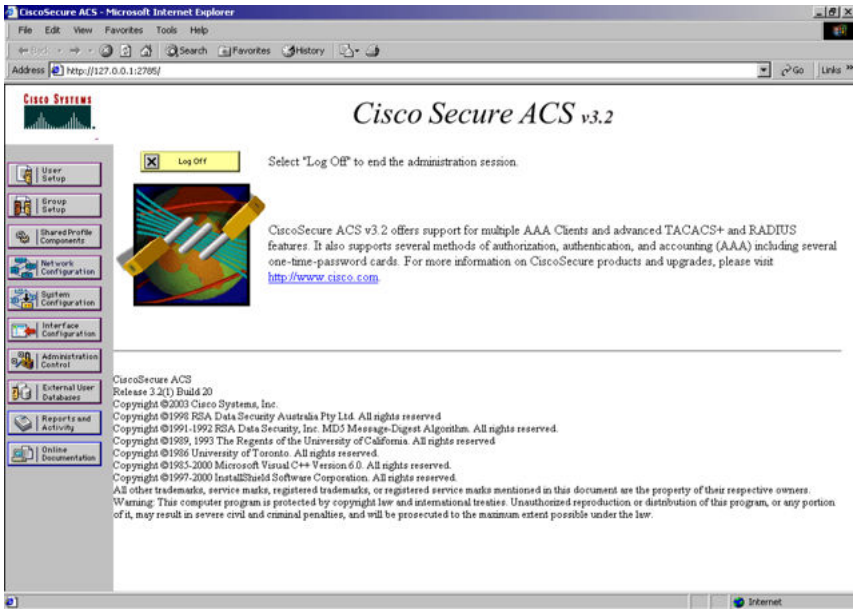
Related Links

TACACS+ configuration examples on page 203

TACACS+ configuration example: Cisco ACS (version 3.2) server

This section provides an example of steps required to configure Cisco ACS (version 3.2) server to function as a TACACS+ server.

The following figure displays the Cisco ACS server main administration window.

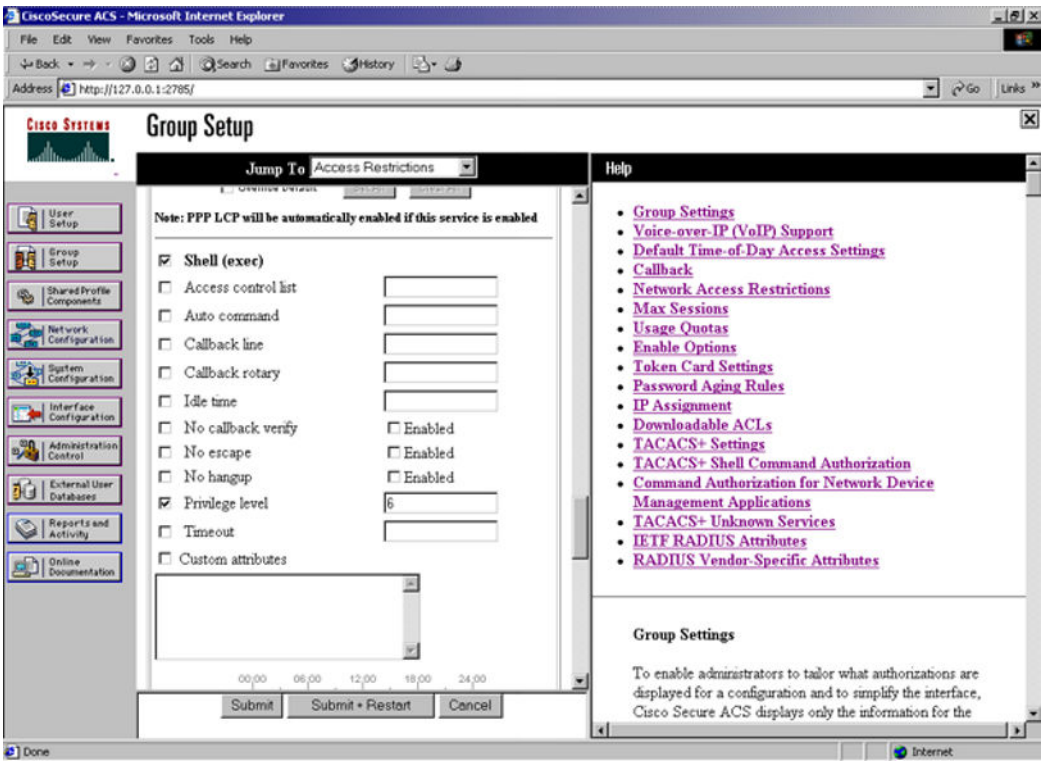


Procedure steps

1. Define the users and the corresponding authorization levels.

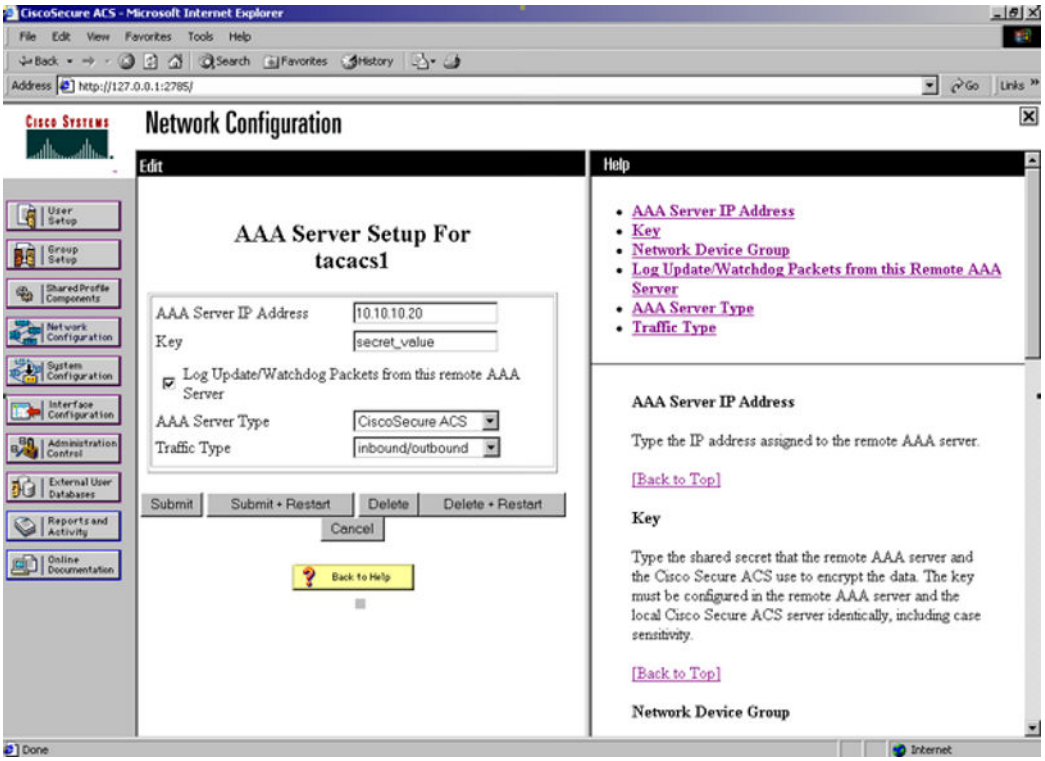
   If you map users to default group settings, remembering which user belongs to each group is easier. For example, the **rwa** user belongs to group 15 to match Privilege level 15. All **rwa** user settings are picked up from group 15 by default.

   The following figure shows a sample Cisco ACS server Group Setup window.



2. Configure the server settings.

   The following figure shows a sample Cisco ACS server Network Configuration window for configuring the authentication, authorization, and accounting (AAA) server for TACACS+.

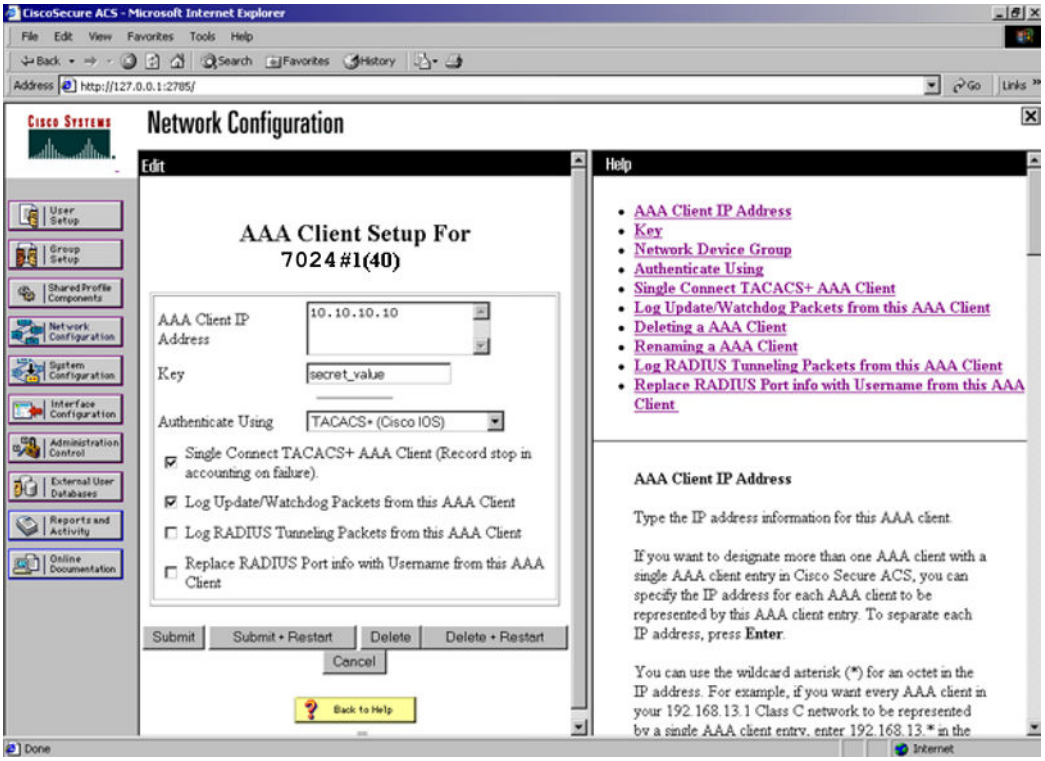


3. Define the client.

   The following figure shows an example of the Cisco ACS server Network Configuration window you can use to configure the client. Authenticate using TACACS+.

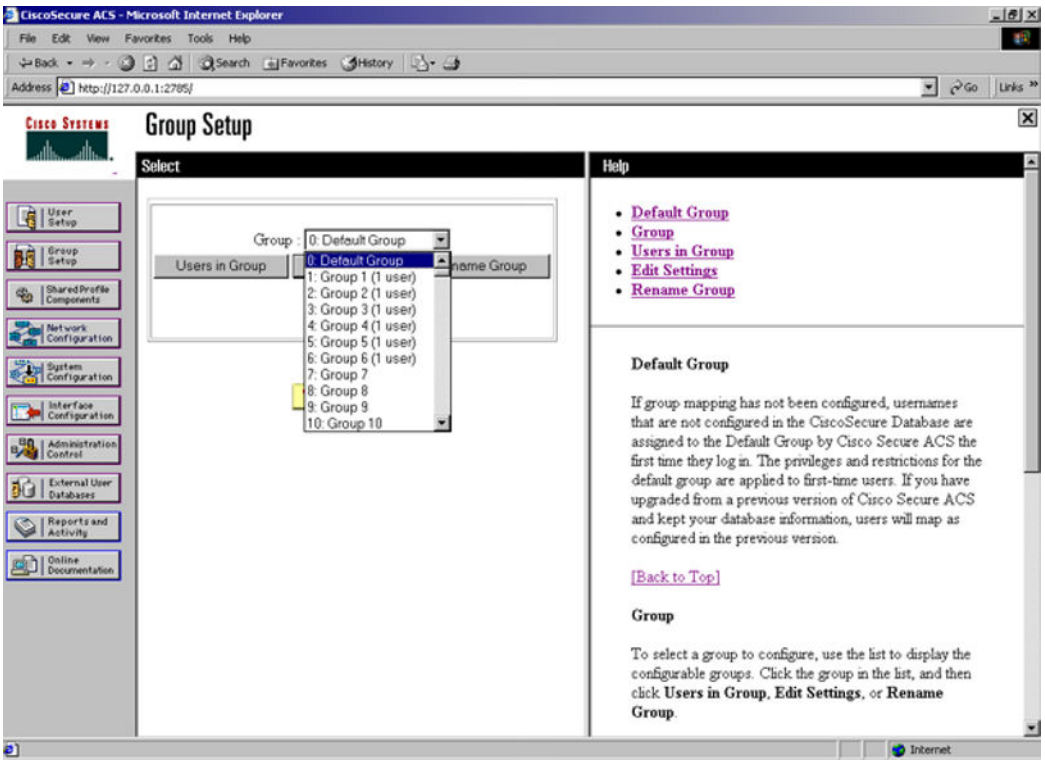
   Note:

   You can use single-connection, but this must match the configuration on the Avaya Virtual Services Platform 7000 Series.

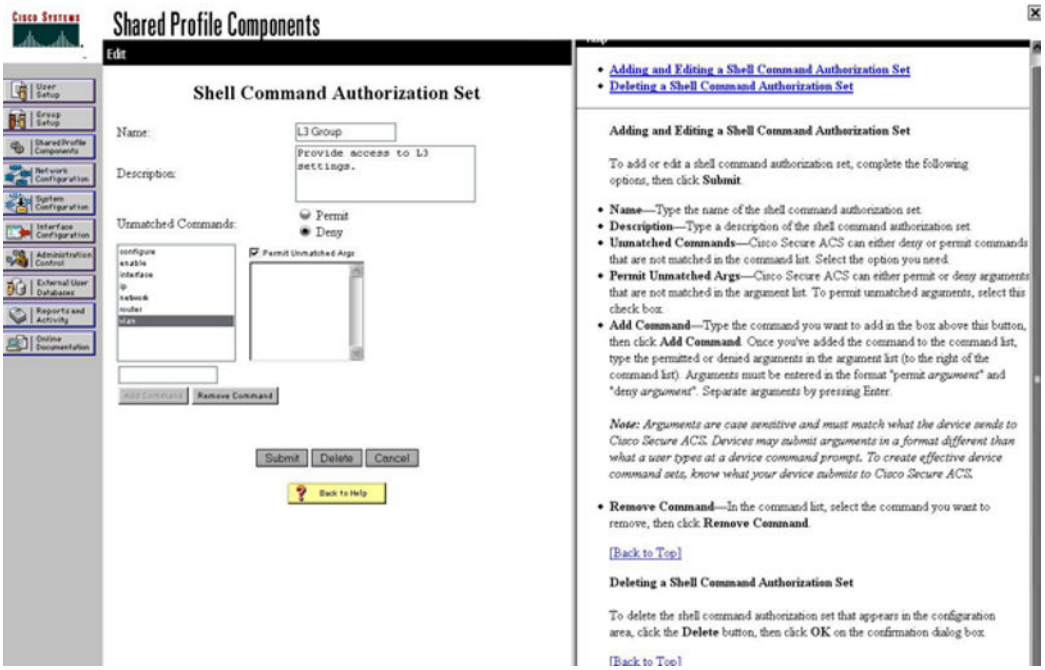


4. Verify the groups you have configured.

   In the example shown in the following figure, the user is associated with a user group. The **rwa** account belongs to group 15, and its privilege level corresponds to the settings for group 15. The **ro** accounts belong to group 0 and **L1** accounts belong to group 2.

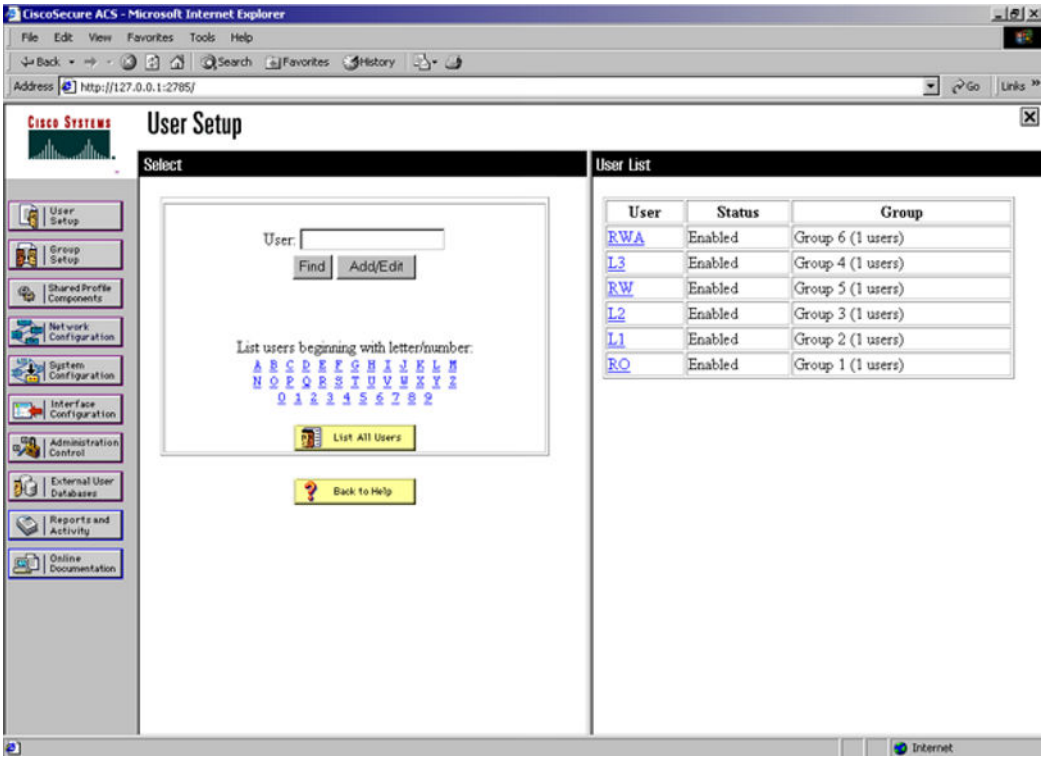


5. Specify the commands allowed or denied for the various groups.
   a. Go to **Shared Profile Components, Shell Command Authorization Set**. The Shell Command Authorization Set screen appears as shown in the following figure.
   b. Select the commands to be added to the command set, and specify whether the action is **permit** or **deny**.



6. View users, user status, and the corresponding group to which each user belongs.

   The following figure shows a sample User Setup window. You can use this window to find, add, edit, and view users settings.



Related Links

TACACS+ configuration examples on page 203

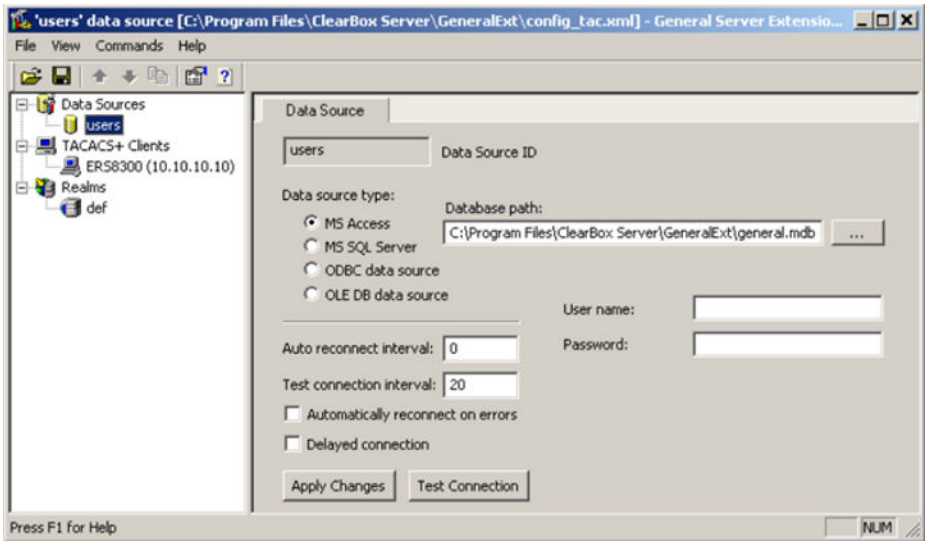
TACACS+ configuration example: ClearBox server

This section provides an example of steps required to configure a ClearBox server to function as a TACACS+ server.

Procedure steps

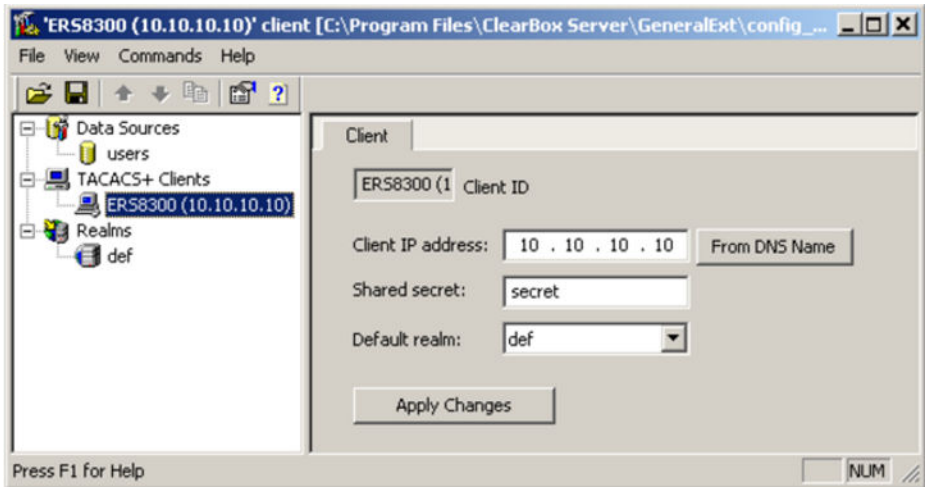
1. Run the General Extension Configurator and configure the user data source as shown in the following figure.

   In this example, Microsoft Access was used to create a database of user names and authorization levels; the *general.mdb* file must include these users.

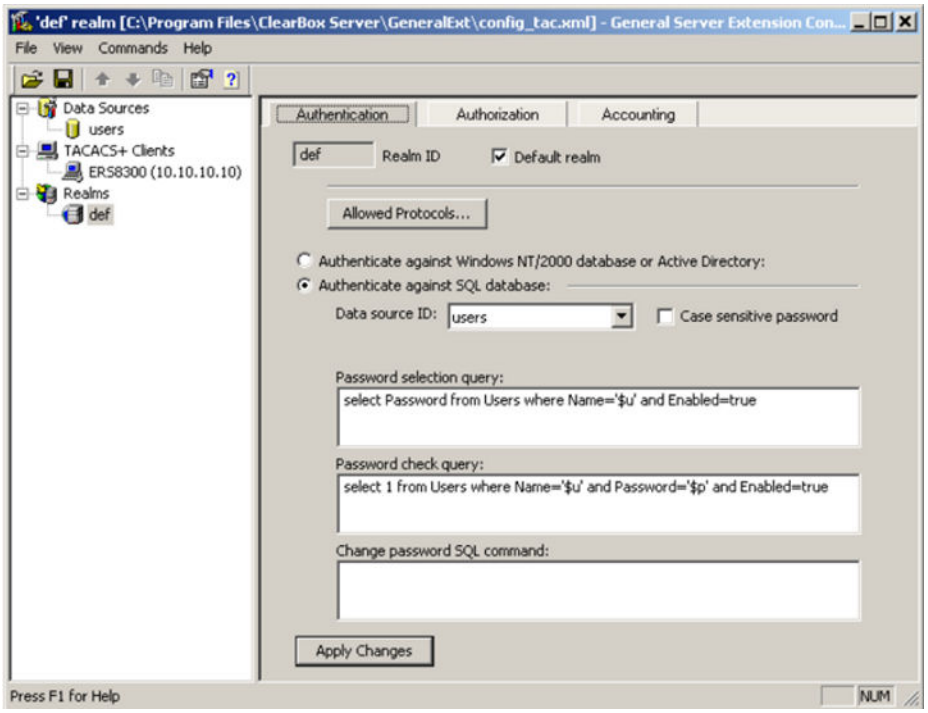


2. Create a Client entry for the switch management IP address by right-clicking the **TACACS+ Clients** item.

   In this case, the TACACS+ Client is the Avaya Virtual Services Platform 7000 Series. Enter the appropriate information. The shared secret must match the value configured on the Avaya Virtual Services Platform 7000 Series.



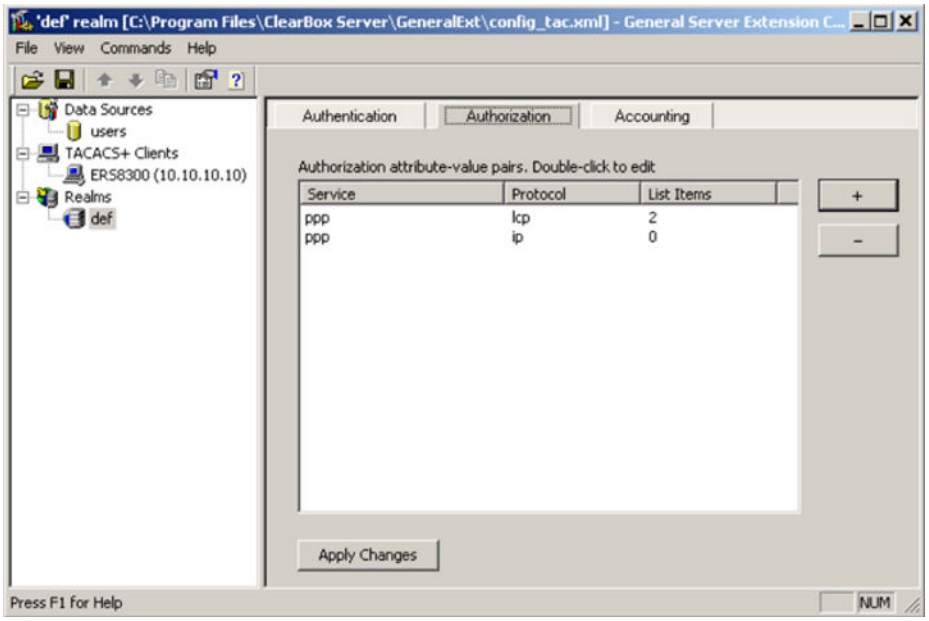
   The default realm Authentication tab looks like the following figure.



3. Click the **Realms, def, Authorization** tab.

   A new service is required that allows the server to assign certain levels of access.

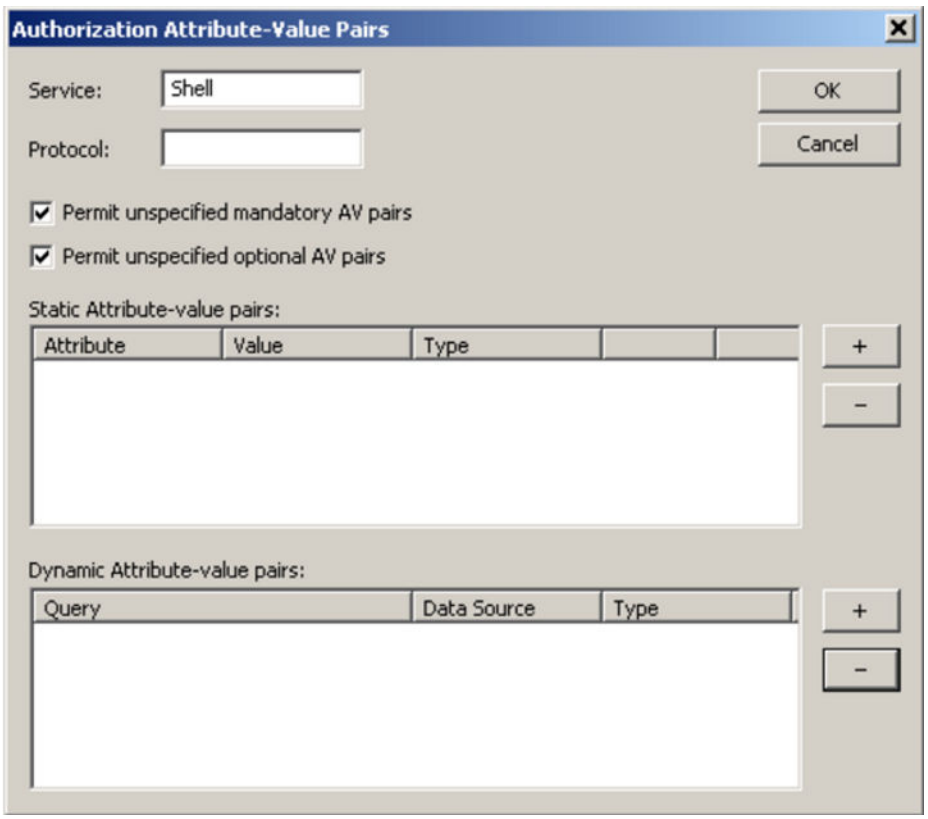
4. Click **+** to add an attribute-value pair for privilege levels (see the following figure).



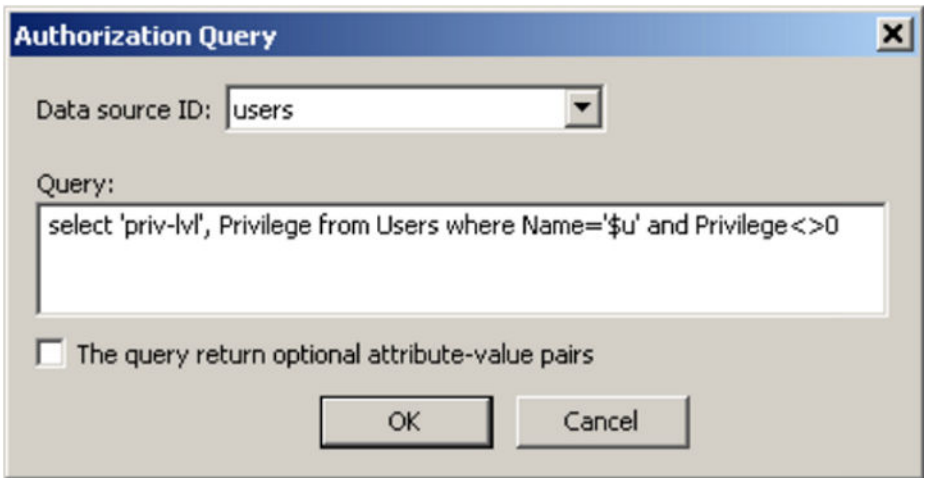
5. Specify the query parameters.

   a. Enter information in the window as shown in the following figure.

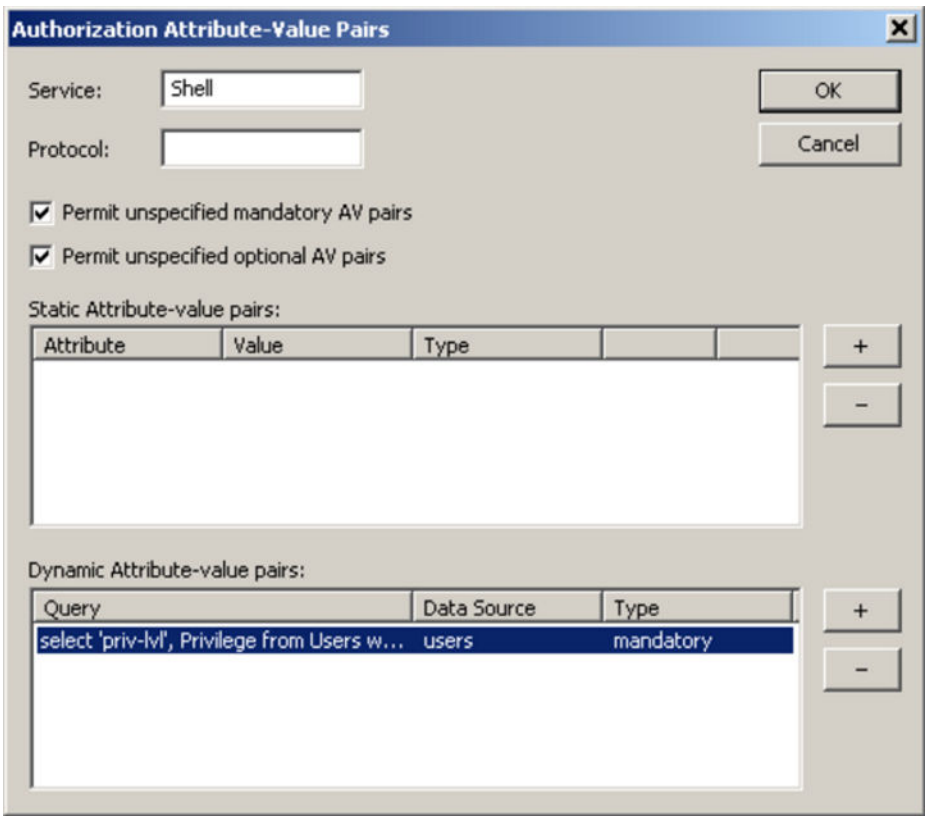
   b. Click **+** to add the parameters to the query.



6. Use the string shown in the following figure for the authorization query.

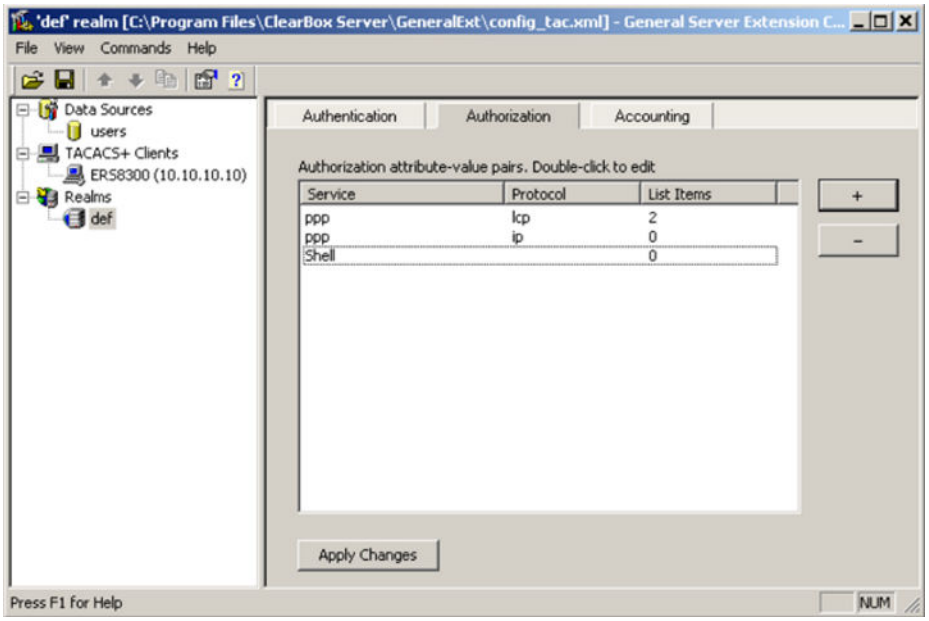


The final window looks like the following figure.



7. Click **OK**.

   The information appears on the Authorization tab (see the following figure).

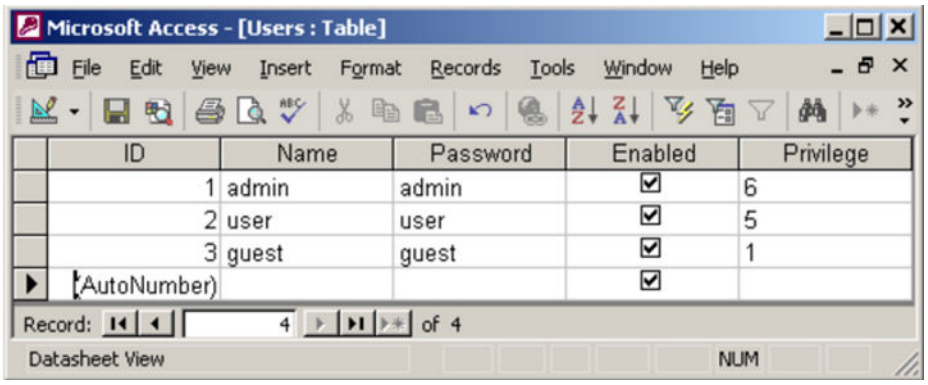


8. Navigate to the *general.mdb* file as specified earlier.

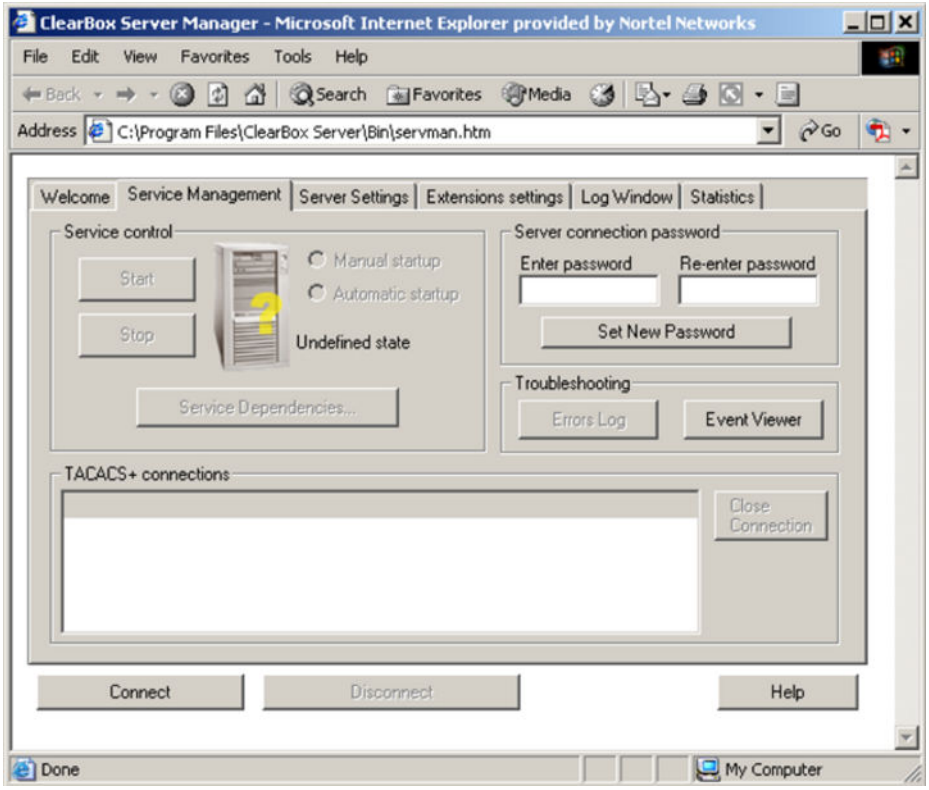
The user table should look like the one shown in the following figure. If the Privilege column does not exist, create one and populate it according to the desired access level.

Important:

If you use the 30-day demo for ClearBox, the user names cannot be more than four characters in length.



9. Start the server.
   a. Run the Server Manager (see the following figure).



   b. Click **Connect**.

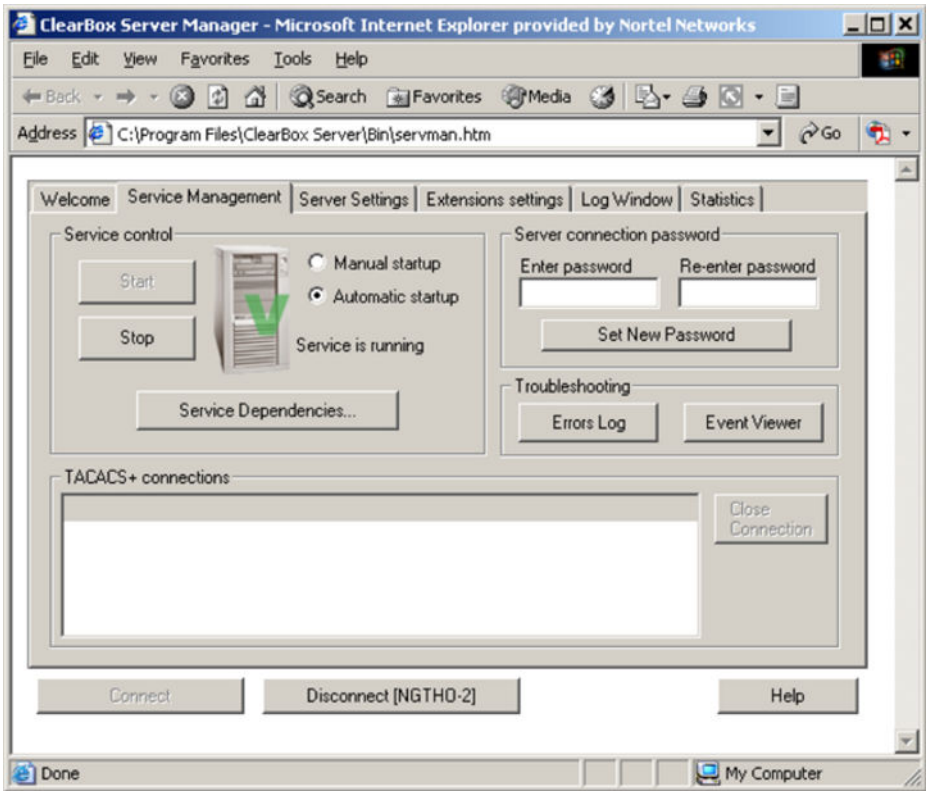
      The **Connect to...** dialog box appears (see the following figure).

c. Click **OK** (do not fill in fields).

d. Click **OK** at the warning message.

e. Click **Start**.

The Server Manager should now look like the following figure. Any changes to the General Server Extension Configurator require restarting the server.



Related Links

TACACS+ configuration examples on page 203

TACACS+ configuration example: Linux freeware server

This section provides an example of steps required to configure a Linux freeware server to function as a TACACS+ server.

Procedure steps

1. After installing TACACS+ on the Linux server, change the directory to:

   ```
   $cd /etc/tacacs
   ```

2. Open the configuration file **tac_plus.cfg**:

   ```
   $vi tac_plus.cfg
   ```

3. Comment out all the existing lines in the configuration file. Add the following lines:

   ```
   # Enter your NAS key and user name key = <secret key> user = <user
   name> {default service = permit service = exec { priv-lvl =
   <Privilege level 1 to 15> } login = <Password type> <password>}
   # Set the location to store the accounting
   records
   ```

   Where:

   - <*secret key*> is the key that you configure on the switch while creating the TACACS+ server entry.
   - <*user name*> is the user name used to log on to the switch.
   - <*Privilege level*> specifies the privilege level (for example, rwa = 6; rw = 5; ro = 1).
   - <*Password type*> specifies the type of password (for example, the password can be clear text or from the Linux password file).
   - <*Password*> if the password type is clear text, this is the password itself.

   The following is a sample config file.

   ```
   $vi tac_plus.cfg


   # Created by Joe SMITH(jsmit@isp.net)
   # Read user_guide and tacacs+ FAQ for more information
   #
   # Enter your NAS key
   key = secretkey
   user = smithJ {
   default service = permit
   service = exec {
   priv-lvl = 15
   }
   login = cleartext M5xyH8
   ```

4. Save the changes to the **tac_plus.cfg** file.
5. Run the TACACS+ daemon using the following command:

   ```
   $/usr/local/sbin/tac_plus -C /etc/tacacs/tac_plus.cfg &
   ```

   Where:

   - *tac_plus* is stored under **/usr/local/sbin**.

- the config file you edited is stored at **/etc/tacacs/**.

The TACACS+ server on Linux is ready to authenticate users.

Related Links

TACACS+ configuration examples on page 203