



Avaya Virtual Services Platform 4000 Administration

Release 5.1.2
NN46251-600
Issue 14.01
January 2017

© 2013-2017, Avaya, Inc.
All Rights Reserved.

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" 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.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR

IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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 is the software contained within the list of Heritage Nortel Products located at <https://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 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

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 products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE

WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <https://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: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

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, its licensors, its suppliers, 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.

Contents

Chapter 1: Introduction	10
Purpose.....	10
Related resources.....	10
Support.....	13
Chapter 2: New in this document	15
Features.....	15
Chapter 3: Basic administration procedures using ACLI	18
Calculating and verifying the md5 checksum	18
Upgrading the software.....	19
Important upgrade consideration.....	22
Deleting a software release.....	23
Saving the configuration.....	24
Saving a file to an external USB device.....	26
Backing up and restoring the compact flash to an external USB device.....	27
Copying configuration and log files to or from a USB device.....	29
Displaying content of a USB file.....	30
Moving a file to or from a USB device.....	31
Deleting a file from a USB device.....	32
Restarting the platform.....	33
Resetting the platform.....	34
Shutting down VSP 4000.....	35
Pinging an IP device.....	36
Calculating the MD5 digest.....	38
Resetting system functions.....	40
Sourcing a configuration.....	41
Chapter 4: Basic administration procedures using EDM	43
Resetting the platform.....	43
Showing the MTU for the system.....	43
Displaying storage use.....	44
Displaying flash file information.....	44
Displaying USB file information.....	45
Displaying USB file information on a card.....	46
Copying a file.....	46
Saving the configuration.....	47
Chapter 5: System startup fundamentals	50
spbm-config-mode boot flag.....	50
Boot sequence.....	50
Configuration redundancy.....	54
System flags.....	54

System connections.....	55
Client and server support.....	55
Chapter 6: Boot parameter configuration using ACLI.....	57
Modifying the boot sequence.....	57
Configuring the remote host logon.....	58
Enabling remote access services.....	59
Changing the primary or secondary boot configuration files.....	63
Configuring system flags.....	64
Configuring serial port devices.....	69
Displaying the boot configuration.....	70
Chapter 7: Run-time process management using ACLI.....	72
Configuring the date.....	72
Configuring the time zone.....	73
Variable definitions.....	73
Configuring the run-time environment.....	74
Configuring the logon banner.....	77
Configuring the message-of-the-day.....	78
Configuring ACLI logging.....	79
Configuring system parameters.....	81
Configuring system message control.....	82
Extending system message control.....	83
Chapter 8: Chassis operations fundamentals.....	85
Software lock-up detection.....	85
Jumbo frames.....	85
SynOptics Network Management Protocol.....	86
10/100/1000BASE-TX Auto-Negotiation recommendations.....	86
CANA.....	87
Auto MDIX.....	88
Chapter 9: Chassis operations configuration using ACLI.....	89
Enabling jumbo frames.....	89
Configuring port lock.....	90
Configuring SONMP.....	91
Viewing the topology message status.....	92
Associating a port to a VRF instance.....	93
Configuring Ethernet ports with Autonegotiation.....	94
Configuring serial management port dropping.....	96
Enabling or disabling the USB port.....	97
Chapter 10: Chassis operations configuration using EDM.....	98
Editing system information.....	98
Editing chassis information.....	99
Configuring system flags.....	101
Configuring basic port parameters.....	102
Changing the boot configuration.....	106

Viewing the boot configuration.....	108
Enabling Jumbo frames.....	110
Associating a port to a VRF instance.....	110
Configuring the date and time.....	111
Auto reactivating the port of the SLPP shutdown.....	111
Editing serial port parameters.....	112
Enabling port lock.....	113
Locking a port.....	113
Viewing power information.....	114
Viewing fan information.....	115
Viewing USB information.....	115
Viewing topology status information.....	116
Viewing the topology message status.....	116
Configuring a forced message control pattern.....	117
Chapter 11: Power over Ethernet fundamentals.....	119
PoE overview.....	119
PoE detection types.....	120
Power usage threshold.....	121
Port power limit.....	121
Port power priority.....	121
Chapter 11: PoE/PoE+ Allocation Using LLDP.....	123
Chapter 12: Power over Ethernet configuration using ACLI.....	124
Disable PoE on a port	124
Configuring PoE detection type.....	125
Configuring PoE power usage threshold.....	126
Configuring power limits for channels.....	126
Configuring port power priority.....	127
Displaying PoE main configuration.....	128
Displaying PoE port status.....	128
Displaying port power measurement.....	129
Chapter 13: Power over Ethernet configuration using EDM.....	131
Configuring PoE globally.....	131
Viewing PoE information for specific switch ports using EDM.....	133
Chapter 14: Hardware status using EDM.....	135
Configuring polling intervals.....	135
Viewing power supply parameters.....	136
Viewing temperature on the chassis.....	136
Chapter 15: DNS fundamentals.....	138
Chapter 16: DNS configuration using ACLI.....	139
Configuring the DNS client.....	139
Querying the DNS host.....	140
Chapter 17: DNS configuration using EDM.....	142

Configuring the DNS client.....	142
Querying the DNS host.....	143
Chapter 18: Licensing fundamentals.....	144
Feature licensing.....	144
License type and part numbers.....	146
Feature license files.....	147
Transition to PLDS.....	147
Chapter 19: License installation using ACLI.....	150
Installing a license file.....	150
Showing a license file.....	152
Chapter 20: License installation using EDM.....	154
Installing a license file.....	154
Chapter 21: NTP fundamentals.....	157
Overview.....	157
NTP system implementation model.....	157
Time distribution within a subnet.....	158
Synchronization.....	159
NTP modes of operation.....	159
NTP authentication.....	160
Chapter 22: NTP configuration using ACLI.....	161
Enabling NTP globally.....	163
Variable definitions.....	164
Adding an NTP server.....	164
Configuring authentication keys.....	165
Chapter 23: NTP configuration using EDM.....	167
Enabling NTP globally.....	169
Adding an NTP server.....	169
Configuring authentication keys.....	170
Chapter 24: Secure Shell fundamentals.....	172
SSH rekeying.....	183
Chapter 25: Secure Shell configuration using ACLI.....	184
Enabling the SSH server.....	184
Changing the SSH server authentication mode.....	185
Configuring SSH configuration parameters.....	185
Verifying and displaying SSH configuration information.....	191
Connecting to a remote host using the SSH client.....	192
Generating user key files.....	192
Managing an SSL certificate.....	195
Disabling SFTP without disabling SSH.....	196
Enabling SSH rekey.....	196
Configuring SSH rekey data-limit.....	197
Configuring SSH rekey time-interval.....	198

Displaying SSH rekey information.....	198
Downgrading or upgrading from releases that support different key sizes.....	199
Chapter 26: Secure Shell configuration using Enterprise Device Manager.....	201
Downloading software from the Avaya support site.....	201
Changing Secure Shell parameters.....	202
Chapter 27: System access fundamentals.....	206
Logging on to the system.....	206
Managing the system using different VRF contexts.....	209
ACLI passwords.....	209
Access policies for services.....	210
Web interface passwords.....	210
Enhanced secure mode authentication access levels.....	211
Password requirements.....	212
Chapter 28: System access configuration using ACLI.....	215
Enabling ACLI access levels.....	215
Changing passwords.....	216
Configuring an access policy.....	218
Specifying a name for an access policy.....	222
Allowing a network access to the switch.....	223
Configuring access policies by MAC address.....	223
System access security enhancements.....	224
Enabling enhanced secure mode.....	225
Displaying the boot config flags status.....	226
Creating accounts for different access levels.....	228
Deleting accounts in enhanced secure mode.....	229
Configuring a password for a specific user.....	230
Returning the system to the factory defaults.....	231
Configuring the password complexity rule.....	232
Configuring the password length rule.....	233
Configuring the change interval rule.....	234
Configuring the reuse rule.....	235
Configuring the maximum age rule.....	236
Configuring the pre- and post-notification rule.....	238
Chapter 29: System access configuration using EDM.....	241
Configuring CLI access using EDM.....	241
Enabling access levels.....	241
Changing passwords.....	242
Configuring the logon banner.....	242
Creating an access policy.....	243
Enabling an access policy.....	247
System access security enhancements using EDM.....	247
Enabling enhanced secure mode.....	247
Chapter 30: ACLI show command reference.....	249

Access, logon names, and passwords.....	249
Basic switch configuration.....	250
Current switch configuration.....	250
CLI settings.....	251
Ftp-access sessions.....	252
Hardware information.....	252
NTP server statistics.....	255
Power summary.....	256
Power information for power supplies.....	256
System information.....	257
System status (detailed).....	259
Telnet-access sessions.....	260
Users logged on.....	260
Port egress COS queue statistics.....	260
CPU queue statistics.....	261
Chapter 31: Port numbering and MAC address assignment reference.....	262
Port numbering.....	262
Interface indexes.....	265
MAC address assignment.....	265
Chapter 32: Supported standards, RFCs, and MIBs.....	267
Supported IEEE standards.....	267
Supported RFCs.....	268
Quality of service.....	271
Network management.....	272
MIBs.....	273
Standard MIBs.....	273
Proprietary MIBs.....	276

Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

This administration guide provides conceptual information and procedures that you can use to administer base system-level topics such as Domain Name Server, network clock synchronization, and Network Time Protocol. It also describes tasks related to the administration of the network including configuration and management of systems, data, and users.

This document includes both initial and ongoing administrative tasks for the Avaya Virtual Services Platform 4000 Series.

For information on administering the Avaya Virtual Services Platform 7200 Series and 8000 Series switches, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Related resources

Documentation

See the *Documentation Roadmap for Avaya Virtual Services Platform 4000 Series*, NN46251-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.Avaya-learning.com.

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 <http://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.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.

5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

GENERAL NOTIFICATIONS

1/5 Notifications Selected

End of Sale and/or Manufacturer Support Notices	<input type="checkbox"/>
Product Correction Notices (PCN)	<input checked="" type="checkbox"/>
Product Support Notices	<input type="checkbox"/>
Security Advisories	<input type="checkbox"/>
Services Support Notices	<input type="checkbox"/>

UPDATE >>

6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

PRODUCT NOTIFICATIONS

Add More Products

Show Details

1 Notices

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.

The screenshot shows two side-by-side panels. The left panel, titled 'PRODUCTS', has a 'My Notifications' link in the top right. It contains a list of products: Virtual Services Platform 7000, Virtualization Provisioning Service, Visual Messenger™ for OCTEL® 250/350, Visual Vectors, Visualization Performance and Fault Manager, Voice Portal, Voice over IP Monitoring, W310 Wireless LAN Gateway, WLAN 2200 Series, and WLAN Handset 2200 Series. The right panel is titled 'VIRTUAL SERVICES PLATFORM 7000' and features a 'Select a Release Version' dropdown menu set to 'All and Future'. Below this are several checkboxes for documentation categories: Administration and System Programming, Application Developer Information, Application Notes, Application and Technical Notes (checked), Declarations of Conformity, and Documentation Library (checked). A red 'SUBMIT >>' button is located at the bottom right of the right panel.

11. Click **Submit**.

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 document

The following sections detail what is new in *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

Features

See the following sections for information about feature changes.

Release 5.1.2

The following features are included in Release 5.1.2:

Logon banner

This release provides the option to set up a custom logon banner using EDM. The logon banner is used to display custom text such as warning message, company name, and contact information to the CLI user before authentication. Until this release, setting up custom warning text was possible only using CLI commands.

For more information, see [Enabling access levels using EDM](#) on page 241.

SSH key sizes

This release updates SSH key sizes. This release accepts key sizes in multiples of 1024. The current key sizes are as follows:

Parameter	Value
DSA host key	1024
RSA host key	1024 or 2048
DSA user key	1024

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the .ssh directory and generate new keys for SSH. For more information about supported software, see *Release Notes for VSP Operating System Software*, NN47227-401.

For more information, see:

- [Secure Shell fundamentals](#) on page 172.
- [Configuring SSH configuration parameters](#) on page 185.
- [Generating user key files](#) on page 192.

- [Downgrading or upgrading from releases that support different key sizes](#) on page 199.
- [Changing Secure Shell parameters](#) on page 202.

SSH parameters

This release updates Secure Shell (SSH) parameters. You can now configure the SSH authentication-type, the SSH encryption-type, and the SSH key-exchange method, using the following commands:

- `ssh authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]}`
- `ssh encryption-type {[3des-cbc] [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [aes128-cbc] [aes128-ctr] [aes192-cbc] [aes192-ctr] [aes256-cbc] [aes256-ctr] [blowfish-cbc] [rijndael128-cbc] [rijndael192-cbc]}`
- `ssh key-exchange-method {[diffie-hellman-group1-sha1] [diffie-hellman-group14-sha1]}`

If you want to delete all authentication, encryption, or key-exchange methods at once use the no parameter before the main command: `no ssh authentication-type`, `no ssh encryption-type`, `no ssh key-exchange-method`.

For more information, see:

- [Secure Shell fundamentals](#) on page 172
- [Configuring SSH configuration parameters](#) on page 185.
- [Changing Secure Shell parameters](#) on page 202.

Enable SSH

To enable SSH, enable RSA or DSA authentication, or both using command `ssh rsa-auth` or `ssh dsa-auth`.

For more information, see:

- [Secure Shell fundamentals](#) on page 172
- [Enabling the SSH server using ACL](#) on page 184
- [Enabling the SSH server using EDM](#) on page 184

Secure web server with TLS

This release introduces the Secure Web server with TLS feature which enhances communications security by replacing the SSL 3.0 protocol with Mocana NanoSSL to secure the HTTP server using the Transport Layer Security (TLS) cryptographic protocol.

TLS server generates a new self-signed certificate on boot and uses that by default. The self-signed certificate is available in `/.intflash/.cert/.ssl`. You can choose to use an online or offline CA signed certificate which will take precedence over the self-signed one.

For more information, see:

- [SSL certificates](#) on page 182
- [Managing SSL certificate](#) on page 195

Release 5.1.1

The following features are included in Release 5.1.1:

RMON1

This release supports RMON1 so RFC2819 was added to [Supported standards RFCs and MIBs](#) on page 267. RMON2 was already supported in a previous release.

Chapter 3: Basic administration procedures using ACLI

The following section describes common procedures that you use while you configure and monitor Avaya Virtual Services Platform 4000 Series operations.

*** Note:**

Unless otherwise stated, to perform the procedures in this section, you must log on to the Privileged EXEC mode in Avaya Command Line Interface (ACLI). For more information about how to use ACLI, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.

*** Note:**

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Calculating and verifying the md5 checksum

Perform this procedure on a Unix or Linux machine to verify that the software files downloaded properly to the switch.

About this task

Calculate and verify the md5 checksum after you download software files.

Procedure

1. Calculate the md5 checksum of the downloaded file:

```
$ /usr/bin/md5sum <downloaded software-filename>
```

Typically, downloaded software files are in the form of compressed Unix file archives (.tgz files).

2. Verify the md5 checksum of the software suite:

```
$ more <md5-checksum output file>
```

- Compare the output that appears on the screen. Ensure that the md5 checksum of the software suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

Calculate the md5 checksum of the downloaded file:

```
$ /usr/bin/md5sum VSP4K.4.1.0.0.tgz
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.1.0.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.1.0.0.zip
a04e7c7cef660bb412598574516c548f VSP4000v4100_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.1.0.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.1.0.0_mib_sup.txt
c5f84beaf2927d937fcbce9dd4d4c7795 VSP4K.4.1.0.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.1.0.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.1.0.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.1.0.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.1.0.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

Upgrading the software

Perform this procedure to upgrade the software on the switch. This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

Use one of the following options to upload the file with the new software to the switch:

- Use FTP or SFTP to transfer the file.
- Download the file to your computer. Copy the file to a USB device and insert the USB device into the USB port on the switch.

Important:

For VSP 4850, the use of the USB port for file transfers using removable FLASH drive is not supported because the USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation.

You can store up to six software releases on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed to add and activate a new software release.

For information about how to remove a software release, see [Deleting a software release](#) on page 23.

Before you begin

- To obtain the new software, go to the Avaya support site: www.avaya.com/support. You need a valid user or site ID and password.
- Back up the configuration files.
- Use an FTP or SFTP application or USB device to transfer the file with the new software release to the switch.
- Ensure that you have not configured a VLAN above 4059. If you have, you must port all configuration on this VLAN to another VLAN, before you begin the upgrade.

Caution:

Starting from Release 3.1, only VLAN range 2 to 4059 is supported. All configuration on a higher numbered VLAN from previous releases will be lost after the upgrade.

- Check the MACsec configuration on the device prior to upgrading to Release 5.0. For more information, see [Important upgrade consideration](#) on page 22.
- If you plan to upgrade from either Release 4.2.1.0 or 4.2.1.1 to 5.0 and have IS-IS-enabled links with HMAC-MD5 authentication, use the `no isis hello-auth` command to disable IS-IS authentication one link at a time for all systems. Ensure each link is stable before you move on to the next link. After you have disabled all IS-IS authentication, save the configuration, and then perform the upgrade to 5.0. After the upgrade to 5.0 is complete, you can reenabling IS-IS authentication one link at a time, and then save the configuration on each switch.
- While upgrading to a release that does not support the same SSH key size, you must delete all of the keys from the `.ssh` directory and generate new keys for SSH.

Note:

Software upgrade configurations are case-sensitive.

About this task

Important:

When both IPv6 `dhcp-relay fwd-path` and IPv6 VRRP are configured on a device that runs 4.1 or 4.2 and you save the configuration, the configuration is saved with an `exit` command missing. This omission prevents the DHCP Relay configuration from loading while rebooting or sourcing the configuration. This issue is fixed in Release 4.2.1, however the omission still exists in configuration files saved using 4.1 or 4.2. As a result, if you upgrade from Release 4.1 or 4.2 to 4.2.1 or later with IPv6 VRRP and IPv6 DHCP configured, the IPv6 DHCP configurations will be lost. After the upgrade, reconfigure IPv6 VRRP- and IPv6 DHCP-related parameters, and then save the configuration. The newer release configuration includes the additional `exit` command when saved.

Procedure

1. Enter Global Configuration mode:

```
enable  
  
configure terminal
```

2. If you are using the USB port to transfer files, go to the next step. If you are using FTP or SFTP to download the files, start the FTP daemon on the switch and enable the `ftpd` flag for FTP or `sshd` flag for SFTP:

*** Note:**

Start an FTP session from your computer to the VSP switch using the same username and password used to Telnet or SSH to the switch. Upload or copy the VOSS image (e.g. VOSS4K.5.0.0.0.tgz) to the VSP switch.

```
boot config flag <ftpd | sshd>
end
```

3. Download the files to the switch through FTP or SFTP, or transfer them to the switch through the USB port.

4. Enter Privileged EXEC configuration mode by exiting the Global Configuration mode.

```
exit
```

5. Extract the release distribution files to the `/intflash/release/` directory:

```
software add WORD<1-99>
```

6. Install the image:

```
software activate WORD<1-99>
```

7. Restart the switch:

```
reset
```

! Important:

After you restart the system, you have the amount of time configured for the commit timer to verify the upgrade and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer has expired. This feature ensures you can regain control of the system if an upgrade fails. By default, auto-commit is enabled.

8. After you restart the switch, enter Privileged EXEC configuration mode:

```
rwa
```

```
enable
```

9. Confirm the software is upgraded:

```
show software
```

10. Commit the software:

```
software commit
```

Example

The following example is for the VSP 8000, but the same steps apply to other VOSS switches.

```
Switch:1>enable
```

```
Switch:1#configure terminal
```

```
Switch:1(config)#boot config flags ftpd
```

Basic administration procedures using ACLI

```
Switch:1(config)#end
Switch:1(config)#copy /usb/VOSS8K.5.0.0.0.tgz /intflash/VOSS8K.
5.0.0.0.tgz
Switch:1(config)#exit
Switch:1#software add VOSS8K.5.0.0.0.tgz
Switch:1#software activate VOSS8K.5.0.0.0.GA
Switch:1#reset
Switch:1#show software
=====
software releases in /intflash/release/
=====
VOSS8K.5.0.0.0.GA (Primary Release)
VOSS8K.4.2.1.0.GA (Backup Release)
-----
Auto Commit      : enabled
Commit Timeout   : 10 minutes
Switch:1#show software detail
=====
software releases in /intflash/release/
=====
VOSS8K.4.2.1.0.GA (Backup Release)
  KERNEL          2.6.32_int38
  ROOTFS          2.6.32_int38
  APPFS           VOSS8K.4.2.1.0int012
  AVAILABLE ENCRYPTION MODULES
  3DES
  AES/DES

VOSS8K.5.0.0.0.GA (Primary Release)
  KERNEL          2.6.32_int38
  ROOTFS          2.6.32_int38
  APPFS           VOSS8K.5.0.0.0.GA
  AVAILABLE ENCRYPTION MODULES
  3DES
  AES/DES
-----
Auto Commit      : enabled
Commit Timeout   : 10 minutes

Switch:1#software commit
```

Important upgrade consideration

Starting with VOSS 5.0 release, support for the replay-protect option within MACsec configuration has been removed. The replay-protect option is no longer visible or configurable in VOSS 5.0. If the

replay-protect option has been configured, follow the steps mentioned below to carefully disable replay-protect before you upgrade to VOSS 5.0.

*** Note:**

Replay-protect must be carefully disabled on both ends of the MACsec enabled link.

Use the `show macsec status` command to check if replay-protect has been enabled on any of the interfaces.

For each interface where MACsec replay protect is enabled, perform the following tasks:

1. Disable MACsec replay-protect on the remote end of the MACsec enabled the link.
2. Disable MACsec replay-protect on the local end of the MACsec enabled link.
3. Save the configuration on both nodes.
4. Start the upgrade to VOSS 5.0.

If replay-protect is not disabled on the remote end of the MACsec link prior to the upgrade of the local node to VOSS 5.0, traffic on the MACsec enabled links will be dropped until replay-protect is also disabled on the remote node. As such, it is strongly recommended to follow the above procedure before initiating upgrade to VOSS 5.0.

Deleting a software release

Perform this procedure to remove a software release from the switch.

*** Note:**

There is a limit of six software releases that can be stored on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed with adding and activating a new software release.

Procedure

1. Enter Privileged EXEC configuration mode:

```
enable
```

2. Remove software:

```
software remove WORD<1-99>
```

Example

The following example is for the VSP 4000 switch, but the same steps apply to other VOSS switches.

```
VSP-4450GSX-PWR+:1>enable
```

```
VSP-4450GSX-PWR+:1#software remove VSP4K.4.1.0.0
```

Saving the configuration

After you update the configuration, you must save the changes on the device. Save the configuration to a file to retain the configuration settings.

You must also save configuration before and after a software upgrade. If an error occurs during the upgrade, use the backup configuration files to return the system to its previous state. Avaya recommends that you keep several copies of backup files.

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

* Note:

If you use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), ensure that you enable the FTP or TFTP server.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Save the running configuration:

```
save config
```

* Note:

The `save config` command saves the configuration file with the filename set as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

3. Copy the configuration files to a safe location:

- a. To copy to internal Flash memory, enter:

```
copy /intflash/<filename>.cfg /intflash/<backup_filename>.cfg
```

- b. To copy the file to a specified directory path on another device with IP address `a.b.c.d`, enter:

```
copy /intflash/<filename>.cfg a.b.c.d:/dir/<backup_filename>.cfg
```

4. (Optional) If required, save the configuration to a different filename than that stored as the primary configuration filename in `boot config`. Update `boot config` with the new filenames.

- a. Specify the primary and backup configuration filenames. Enter:

```
save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
```

- b. Update the primary and backup configuration filenames in `boot config`.

*** Note:**

This step is necessary to restore the platform with your configuration file, after a reset.

Enter:

```
boot config choice primary config-file <filename>.cfg
boot config choice primary backup-config-file
<backup_filename>.cfg
```

Example

```
VSP-4850GTS-PWR+:1> enable
```

Determine the current primary configuration and backup configuration filenames:

```
VSP-4850GTS#show boot config choice
choice primary config-file "/intflash/config.cfg"
choice primary backup-config-file "/intflash/config.cfg"
```

Save the running configuration:

```
VSP-4850GTS-PWR+:1# save config
```

Copy the configuration files to a safe location. Enter:

```
VSP-4850GTS#copy /intflash/config.cfg /intflash/config_backup.cfg
VSP-4850GTS#copy /intflash/config.cfg 10.29.140.190/dir/config_backup.cfg
```

(Optional) Save the configuration to filenames of your choice.

```
save config [backup 010.29.140.190/dir/AvayaConfigBackup.cfg] [file
10.29.140.190/dir/AvayaConfig.cfg]
```

(Optional) Update the primary and backup configuration files in `boot config`

```
boot config choice primary config-file AvayaConfig.cfg
boot config choice primary backup-config-file AvayaConfigBackup.cfg
```

Variable definitions

Use the data in the following table to use the `save config` command.

Variable	Value
backup <i>WORD</i> <1–99>	Saves the specified file name and identifies the file as a backup file. <i>WORD</i> <1–99> uses one of the following format: <ul style="list-style-type: none"> a.b.c.d:<file> /intflash/<file>

Table continues...

Variable	Value
	The file name, including the directory structure, can include up to 99 characters.
file <i>WORD</i> <1–99>	Specifies the file name in one of the following format: <ul style="list-style-type: none"> • a.b.c.d:<file> • /intflash/<file> The file name, including the directory structure, can include up to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Saving a file to an external USB device

Use the following procedure to save the configuration file or log file to an external USB device.

 **Important:**

This procedure is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

 **Caution:**

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Procedure

1. Enter Privileged EXEC mode:


```
enable
```
2. Save the file to an external USB device:
 - a. To save the configuration file to an external USB device, enter:


```
save config file WORD<1-99>
```
 - b. To save the log file to an external USB device, enter:


```
save log file WORD<1-99>
```

Example

```
VSP-4450GSX-PWR+:1#save config file /usb/test.cfg
CP-1: Save config to file /usb/test.cfg successful.
WARNING: Choice Primary Node Config file is "/intflash/soak.cfg".

VSP-4450GSX-PWR+:1#
VSP-4450GSX-PWR+:1#save log file /usb/test.log
```



```
Save log to file /usb/test.log successful.
Save log to file /usb/test.log successful.
VSP-4450GSX-PWR+:1#
```

Variable definitions

Use the data in the following table to use the `save` command.

Variable	Value
config file <i>WORD</i> <1-99>	<p>Specifies the software configuration device and configuration file name in one of the following formats:</p> <ul style="list-style-type: none"> • a.b.c.d:<file> • /intflash/<file> • /usb/<file> <p>The file name, including the directory structure, can include up to 99 characters.</p>
log file <i>WORD</i> <1-99>	<p>Specifies the software configuration device and log file name in one of the following formats:</p> <ul style="list-style-type: none"> • a.b.c.d:<file> • /intflash/<file> • /usb/<file> <p>The file name, including the directory structure, can include up to 99 characters.</p>

Backing up and restoring the compact flash to an external USB device

Perform this procedure to back up and restore the contents of the internal compact flash to a USB flash device without entering multiple `copy` commands. This procedure is useful if you want to copy the complete compact flash contents to another chassis.

Note:

The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

Caution:

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Before you begin

You must have a USB storage device ready to use that is at least 2 GB. The switch supports USB 1 and 2.

About this task

The system verifies that the USB flash device has enough available space to perform the backup operation. If the USB flash device does not have enough available space, an error message appears. The backup command uses the following filepath on the USB flash device: `/usb/intflash/intflashbackup_yyyymmddhhmmss.tgz`.

Important:

Disable logging using the command: `no boot config logging`.

The backup action can take up to 10 minutes.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Backup the internal flash to USB:

```
backup intflash
```

3. Restore the data to the internal flash:

```
restore intflash
```

Example

```
Switch:1#backup intflash
```

```
Warning: Command will backup all data from /intflash to /usb/intflash.  
It will take a few minutes and may cause high CPU utilization.
```

```
Are you sure you want to continue? (y/n) ? y
```

```
For file system /intflash:
```

```
7252475904 total bytes on the filesystem  
990920704 used bytes on the filesystem  
6261555200 free bytes on the filesystem
```

```
For file system /usb:
```

```
2021216256 total bytes on the filesystem  
12038144 used bytes on the filesystem  
2009178112 free bytes on the filesystem
```

```
cd /intflash ; /bin/tar -czvf /usb/intflash/intflashbackup_20140610074501.tgz *  
; /bin/sync
```

```
Info: Backup /intflash to filename /usb/intflash/intflashbackup_20140610074501.tgz is  
complete!
```

```
Do you want to stop the usb? (y/n) ? n
```

Copying configuration and log files to or from a USB device

Use the following procedure to copy configuration and log files to an external USB device from the internal Flash memory (Intflash) or TFTP server, or to copy files from an external USB device to the Intflash.

Important:

This procedure is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

Caution:

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Copy the configuration or log files to a safe location:

- a. To copy configuration and log files to an external USB device:

From the internal Flash memory:

```
copy /intflash/<srcfile> /usb/<destfile>
```

From a TFTP server:

```
copy <a.b.c.d>:<srcfile> /usb/<destfile>
```

- b. To copy configuration or log files from the USB device to Intflash:

```
copy /usb/<srcfile> /intflash/<destfile>
```

Example

```
VSP-4450GSX-PWR+:1#enable
VSP-4450GSX-PWR+:1#copy /intflash/test.cfg /usb/test.cfg
VSP-4450GSX-PWR+:1#copy 142.10.0.8:test.cfg /usb/test.cfg
```

```
VSP-4450GSX-PWR+:1#enable
VSP-4450GSX-PWR+:1#copy /usb/test.cfg /intflash/test.cfg
```

Variable definitions

Use the data in the following table to use the `copy` command.

Variable	Value
<a.b.c.d>	Specifies the IPv4 address of the TFTP server from which to copy the license file.
<destfile>	Specifies the name of the configuration or log file when copied to the USB device. The destination file name must be lower case and have a file extension of .cfg or .log. For example, test.cfg or test.log. The file name, including the directory structure, can include up to 255 characters.
<srcfile>	Specifies the name of the configuration or log file on the internal flash memory. For example, test.cfg or test.log. The file name, including the directory structure, can include up to 255 characters.

Displaying content of a USB file

Use the following procedure to view content of a USB file.

Important:

This procedure is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

Caution:

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display content of a USB file:

```
more WORD<1-99>
```

Example

```
VSP-4450GSX-PWR+:1#enable
```

```
VSP-4450GSX-PWR+:1#more /usb/test.cfg
```

Variable definitions

Use the data in the following table to use the `more` command.

Variable	Value
<code>WORD<1–99></code>	Specifies the file name in the following format: <ul style="list-style-type: none"> • <code>/usb/<file></code> The file name, including the directory structure, can include up to 99 characters.

Moving a file to or from a USB device

Use the following procedure to move a file from the internal Flash memory (Intflash) to an external USB device, or from a USB device to Intflash.

Important:

This procedure is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

Caution:

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Procedure

1. Enter Privileged EXEC mode:


```
enable
```
2. Move a file to a safe location:
 - a. To move a file from Intflash to a USB device:


```
mv /intflash/<srcfile> /usb/<destfile>
```
 - b. To move a file from a USB device to Intflash:


```
mv /usb/<srcfile> /intflash/<destfile>
```

Example

```
VSP-4450GSX-PWR+:1#enable
VSP-4450GSX-PWR+:1#mv /intflash/test.cfg /usb/test.cfg
```

```
VSP-4450GSX-PWR+:1#enable
VSP-4450GSX-PWR+:1#mv /usb/test.cfg /intflash/test.cfg
```

Variable definitions

Use the data in the following table to use the `mv` command.

Variable	Value
<destfile>	Specifies the name of the configuration or log file when moved to the USB device. The destination file name must be lower case and have a file extension of <code>.cfg</code> or <code>.log</code> . For example, <code>test.cfg</code> or <code>test.log</code> . The file name, including the directory structure, can include up to 255 characters.
<srcfile>	Specifies the name of the configuration or log file on the internal flash memory. For example, <code>test.cfg</code> or <code>test.log</code> . The file name, including the directory structure, can include up to 255 characters.

Deleting a file from a USB device

Use the following procedure to delete a file from an external USB device.

Important:

This procedure is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.

Caution:

Always use the `usb-stop` command to safely unplug the USB drive from the USB slot.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Delete a file from a USB device:

```
delete WORD<1-255>
```

Example

```
VSP-4450GSX-PWR+:1#enable
VSP-4450GSX-PWR+:1#delete /usb/test.cfg
Are you sure (y/n) ? y
VSP-4450GSX-PWR+:1#
```

Variable definitions

Use the data in the following table to use the `delete` command.

Variable	Value
<code>WORD<1–255></code>	Specifies the file name in the following format: <ul style="list-style-type: none"> • <code>/usb/<file></code>

Restarting the platform

Before you begin

 **Note:**

The command mode is very important for this command. If you are logged on to a different command mode, such as Global Configuration mode, rather than Privileged EXEC mode, different options appear for this command.

About this task

Restart the platform to implement configuration changes or recover from a system failure. When you restart the system, you can specify the boot config file name. If you do not specify a boot source and file, the `boot` command uses the configuration files on the primary boot device defined by the `boot config choice` command.

After the switch restarts normally, it sends a cold trap within 45 seconds after the restart.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. Restart the switch:

```
boot [config WORD<1-99>] [-y]
```

 **Important:**

If you enter the `boot` command with no arguments, you cause the switch to start using the current boot choices defined by the `boot config choice` command.

If you enter a boot command and the configuration file name without the directory, the device uses the configuration file from `/intflash/`.

Example

```
VSP-4850GTS-PWR+:1>enable
```

Restart the switch:

```
VSP-4850GTS-PWR+:1#boot config /intflash/config.cfg  
Are you sure you want to re-boot the switch (y/n) ?y
```

Variable definitions

Use the data in the following table to use the `boot` command.

Table 1: Variable definitions

Variable	Value
config <i>WORD</i> <1–99>	<p>Specifies the software configuration device and file name in one of the following formats:</p> <ul style="list-style-type: none">• a.b.c.d:<file>• /intflash/ <file>• /usb/<file> <p>! Important:</p> <p>Restarting the platform from a USB device is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.</p> <p>The file name, including the directory structure, can include up to 99 characters.</p>
-y	<p>Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the system restarts.</p>

Resetting the platform

About this task

Reset the platform to reload system parameters from the most recently saved configuration file.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Reset the platform:

```
reset [-y]
```


Example

```
VSP-4850GTS-PWR+:1>enable
```

Reset the switch:

```
VSP-4850GTS-PWR+:1#reset
```

```
Are you sure you want to reset the switch? (y/n)y
```

Variable definitions

Use the data in the following table to use the `reset` command.

Table 2: Variable definitions

Variable	Value
-y	Suppresses the confirmation message before the switch resets. If you omit this parameter, you must confirm the action before the system resets.

Shutting down VSP 4000

Use the following procedure to shut down VSP 4000.

⚠ Caution:

Before you unplug the AC power cord, always perform the following shutdown procedure. This procedure flushes any pending data to ensure data integrity.

Procedure

1. Enter the Privileged EXEC configuration mode.

```
enable
```

2. Shut down VSP 4000:

```
sys shutdown
```

Example

```
VSP-4450GSX-PWR+:1>enable
```

```
VSP-4450GSX-PWR+:1#sys shutdown
```

```
Are you sure you want shutdown the system? Y/N (y/n) ? y
```

```
CP1 [03/24/14 18:39:04.932:UTC] 0x00010813 00000000 GlobalRouter HW INFO
System shutdown initiated from CLI
```

```
CP1 [03/24/14 18:39:06.000] LifeCycle: INFO: Stopping all processes
```

Basic administration procedures using ACLI

```
CP1 [03/24/14 18:39:08.000] LifeCycle: INFO: All processes have stopped
CP1 [03/24/14 18:39:08.000] LifeCycle: INFO: All applications shutdown,
starting power down sequence
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none
killed
cat: can't open '/proc/mtd': No such file or directory
cat: can't open '/proc/mtd': No such file or directory
Stopping vsp...
mount: no /proc/mounts
mount: can't find /mnt/cfgfs/ in /etc/fstab
/etc/rc0.d/K25vsp: line 441: /mnt/cfgfs/timestamp: Read-only file system
umount: can't open '/proc/mounts'
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
Deconfiguring network interfaces... done.
Stopping syslogd/klogd: no syslogd found; none killed
Sending all processes the TERM signal...
Sending all processes the KILL signal...
hwclock: can't open '/dev/misc/rtc': No such file or directory
/etc/rc0.d/S25save-rtc.sh: line 5: /etc/timestamp: Read-only file system
Unmounting remote filesystems...
Stopping portmap daemon: portmap.
Deactivating swap...
Unmounting local filesystems...
[695413.959234] Power down.
[695413.989531] System Halted, OK to turn off power
```

Pinging an IP device

About this task

Ping a device to test the connection between Avaya Virtual Services Platform 4000 Series and another network device. After you ping a device, the switch sends an Internet Control Message

Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address does not respond.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Enter the Privileged EXEC mode:

```
enable
```

3. Ping an IP network connection:

```
ping WORD<0-256> [-d] [-I <1-60>] [-s] [-t <1-120>] [count <1-9999>]
[datasize <28-51200>] [interface WORD <1-256>|gigabitEthernet|
tunnel|vlan] [scopeid <1-9999>] [source WORD<1-256>] [vrf WORD<0-
16>]
```

Example

Ping an IP device through the management interface:

```
VSP-4850GTS-PWR+:1#ping 192.0.2.16
192.0.2.16 is alive
```

Variable definitions

Use the data in the following table to use the `ping` command.

Table 3: Variable definitions

Variable	Value
count <1-9999>	Specifies the number of times to ping (1-9999).
-d	Configures the ping debug mode. This variable detects local software failures (ping-related threads creation or write to sending socket) and receiving issues (ICMP packet too short or wrong ICMP packet type).
datasize {28-9216 28-51200}	Specifies the size of ping data sent in bytes. The datasize for IPv4 addresses is <28-9216>. The datasize for IPv6 addresses is <28-51200>. The default is 0.
interface WORD <1-256>	Configures a specific outgoing interface to use by IP address.

Table continues...

Variable	Value
	Additional ping interface filters: <ul style="list-style-type: none"> • gigabitEthernet: {slot/port} gigabit ethernet port • tunnel: tunnel ID as a value from 1–2000 • vlan: VLAN ID as a value from 1–4059
-l <1–60>	Specifies the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the [-l] parameter.
scopeid <1–9999>	Specifies the scope ID. <1–9999> specifies the circuit ID for IPv6.
source WORD<1–256>	Specifies an IP address to be used as the source IP address in the packet header.
-t <1–120>	Specifies the no-answer timeout value in seconds (1–120).
vrf WORD<0–16>	Specifies the virtual routing and forwarding (VRF) name from 1–16 characters.
WORD<0–256>	Specifies the host name or IPv4 (a.b.c.d), or IPv6 (x:x:x:x:x:x) address (string length 0–256). Specifies the address to ping.

Calculating the MD5 digest

Before you begin

- Use the `md5` command with reserved files (for example, a password file) only if you possess sufficient permissions to access these files.

About this task

Calculate the MD5 digest to verify the MD5 checksum. The `md5` command calculates the MD5 digest for files on the internal flash and either shows the output on screen or stores the output in a file that you specify. An `md5` command option compares the calculated MD5 digest with that in a checksum file on flash, and the compared output appears on the screen. By verifying the MD5 checksum, you can verify that the file transferred properly to the switch.

Important:

If the MD5 key file parameters change, you must remove the old file and create a new file.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Enter the Privileged EXEC mode:

```
enable
```

3. Calculate the MD5 digest:

```
md5 WORD<1-99> [-a] [-c] [-f WORD<1-99>] [-r]
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

Add the data to the output file instead of overwriting it:

```
VSP-4850GTS-PWR+:1#md5 password -a
```

Variable definitions

Use the data in the following table to use the `md5` command.

Table 4: Variable definitions

Variable	Value
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by <i>WORD<1-99></i> with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum filename is not specified, the file <code>/intflash/checksum.md5</code> is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: Error: Checksum file <i><filename></i> not present. The -c option also <ul style="list-style-type: none"> • calculates the checksum of files specified by <i>WORD<1-99></i> • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison
-f <i>WORD<1-99></i>	Stores the result of MD5 checksum to a file on internal flash. If the output file specified with the -f option is reserved filenames on the switch, the command fails with the error message: Error: Invalid operation.

Table continues...

Variable	Value
	<p>If the output file specified with the -f option is files for which to compute MD5 checksum, the command fails with the error message:</p> <pre data-bbox="841 344 1464 422">VSP-4850GTS-PWR+:1# md5 *.cfg -f config.cfg Error: Invalid operation on file <filename></pre> <p>If the checksum filename specified by the -f option exists on the switch (and is not one of the reserved filenames), the following message appears on the switch:</p> <pre data-bbox="841 583 1464 632">File exists. Do you wish to overwrite? (y/n)</pre>
-r	<p>Reverses the output. Use with the -f option to store the output to a file.</p> <p>You cannot use the -r option with the -c option.</p>

Resetting system functions

About this task

Reset system functions to reset all statistics counters, the console port.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. Reset system functions:

```
sys action reset {console|counters}
```

Example

```
VSP-4850GTS-PWR+:1> enable
```

Reset the statistics counters:

```
VSP-4850GTS-PWR+:1> sys action reset counters
```

```
Are you sure you want to reset system counters (y/n)? y
```

Variable definitions

Use the data in the following table to use the `sys action` command.

Table 5: Variable definitions

Variable	Value
reset {console counters}	Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console connection does not respond. Resets all the statistics counters in the switch to zero. Resets the console port.

Sourcing a configuration

About this task

Source a configuration file to merge the configuration into the running configuration.

IPv4 and IPv6 addresses are supported with no difference in configuration or functionality.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. Source a configuration:

```
source WORD<1-99> [debug] [stop] [syntax]
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

Debug the script output:

```
VSP-4850GTS-PWR+:1#source testing.cfg debug
```

Variable definitions

Use the data in the following table to use the `source` command.

Table 6: Variable definitions

Variable	Value
debug	Debugs the script output.
stop	Stops the merge after an error occurs.
syntax	Verifies the script syntax.
WORD<1-99>	Specifies a filename and location in one of the following formats: <ul style="list-style-type: none"> • a.b.c.d:<file>

Table continues...

Variable	Value
	<ul style="list-style-type: none"> • /intflash/<file> • /usb/<file> <p>! Important:</p> <p>Sourcing a configuration from a USB device is applicable only to the VSP 4450GSX-PWR+ model of the VSP 4000. The VSP 4850GTS Series has a fixed USB drive configuration and the USB port cannot be used for file transfer.</p> <p><file> is a string. The path and <file> can use 1–99 characters.</p>

Chapter 4: Basic administration procedures using EDM

The following section describes common procedures that you use while you configure and monitor Avaya Virtual Services Platform 4000 Series operations using Enterprise Device Manager (EDM).

Resetting the platform

About this task

Reset the platform to reload system parameters from the most recently saved configuration file. Use the following procedure to reset the device using EDM.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **System** tab.
5. Locate **ActionGroup4** near the bottom of the screen.
6. Select **softReset** from **ActionGroup4**.
7. Click **Apply**.

Showing the MTU for the system

About this task

Perform this procedure to show the MTU configured for the system.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.

3. Click **Chassis**.
4. Click on the **Chassis** tab.
5. Verify the selection for the MTU size.

Displaying storage use

About this task

Display the amount of memory used, memory available, and the number of files for internal flash memory.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **File System**.
3. Click the **Storage Usage** tab.

Device Info field descriptions

Use the data in the following table to use the **Device Info** tab.

Name	Description
FlashBytesUsed	Specifies the number of bytes used in internal flash memory.
FlashBytesFree	Specifies the number of bytes available for use in internal flash memory.
FlashNumFiles	Specifies the number of files in internal flash memory.

Displaying flash file information

About this task

Display information about the files in internal flash memory on this device.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **File System**.
3. Click the **Flash Files** tab.

Flash Files field descriptions

Use the data in the following table to use the **Flash Files** tab.

Name	Description
Slot	Specifies the slot number of the device.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Displaying USB file information

About this task

Display information about the files on a USB device, for each slot on the card, to view general file information.

Caution:

Always use the `usb-stop` command using the ACLI to safely unplug the USB drive from the USB slot.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

USB Files field descriptions

Use the data in the following table to use the **USB Files** tab under **Edit > File System**.

Name	Description
Slot	Specifies the slot number where the CP module is installed.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Displaying USB file information on a card

About this task

Display information about the files on a USB device, for each card, to view general file information.

Caution:

Always use the `usb-stop` command using the ACLI to safely unplug the USB drive from the USB slot.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Card**.
3. Click the **USB Files** tab.

USB Files on a card field descriptions

Use the data in the following table to use the **USB Files** tab under **Edit** > **Card**.

Name	Description
Slot	Specifies the slot number where the card is installed.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Copying a file

About this task

Copy files on the internal flash.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Copy File** tab.
4. Edit the fields as required.
5. Click **Apply**.

Copy File field descriptions

Use the data in the following table to use the **Copy File** tab.

Name	Description
Source	Identifies the source file to copy. You must specify the full path and filename.
Destination	Identifies the device and the file name (optional) to which to copy the source file. You must specify the full path. Trace files are not a valid destination.
Action	Starts the copy process or stops the copy process.
Result	Specifies the result of the copy process: <ul style="list-style-type: none"> • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

Saving the configuration

About this task

After you change the configuration, you must save the changes on the device. Save the configuration to a file to retain the configuration settings.

Note:

When you logout of the EDM interface, a dialogue box automatically prompts if you want to save the configuration. If you want to save the configuration, click **OK**. If you want to close without saving the configuration, click **Cancel**. If you no longer see the prompt, clear your browser cache, restart your browser and reconnect.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.

4. Click the **System** tab.
5. Optionally, specify a filename in **ConfigFileName**.
If you do not specify a filename, the system saves the information to the default file.
6. In **ActionGroup1**, select **saveRuntimeConfig**.
7. Click **Apply**.

System field descriptions

Use the data in the following table to use the **System** tab.

Name	Description
sysDescr	Shows the system assigned name and the software version.
sysUpTime	Shows the elapsed time since the system last started.
sysContact	Configures the contact information (in this case, an email address) for the Avaya support group.
sysName	Configures the name of this device.
sysLocation	Configures the physical location of this device.
DnsDomainName	Configures the default domain for querying the DNS server.
LastChange	Displays the time since the last configuration change.
LastVlanChange	Displays the time since the last VLAN change.
LastStatisticsReset	Displays the time since the statistics counters were last reset.
LastRunTimeConfigSave	Displays the last run-time configuration saved.
DefaultRuntimeConfigFileName	Displays the default Run-time configuration file directory name.
ConfigFileName	Specifies the name of a new configuration file.
ActionGroup1	Can be one of the following actions: <ul style="list-style-type: none"> • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration • loadLicense—loads a software license file to enable features

Table continues...

Name	Description
ActionGroup3	Can be the following action: <ul style="list-style-type: none">• flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be the following action: <ul style="list-style-type: none">• softReset—resets the device without running power-on tests
Result	Displays a message after you click Apply .

Chapter 5: System startup fundamentals

This section provides conceptual material on the boot sequence and boot processes of the Avaya Virtual Services Platform 4000 Series. Review this content before you make changes to the configurable boot process options.

spbm-config-mode boot flag

Shortest Path Bridging (SPB) and Protocol Independent Multicast (PIM) cannot interoperate with each other on the switch at the same time. To ensure that SPB and PIM stay mutually exclusive, a boot flag called `spbm-config-mode` is implemented.

- The `spbm-config-mode` boot flag is enabled by default. This enables you to configure SPB and IS-IS, but you cannot configure PIM either globally or on an interface.
- If you disable the boot flag, save the config and reboot with the saved config. When the flag is disabled, you can configure PIM and IGMP Snooping, but you cannot configure SPB or IS-IS.

Important:

Whenever you change the `spbm-config-mode` boot flag, you should save the configuration and reboot the switch for the change to take effect.

For information about configuring boot flags, see *Configuring system flags* or *Changing the boot configuration* in *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600. For more information about this boot flag and Simplified vIST, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series*, NN46251-504.

Boot sequence

The Virtual Services Platform 4000 goes through a three-stage boot sequence before it becomes fully operational. After you turn on power to the switch, the system starts.

The boot sequence consists of the following stages:

- [Stage 1: Loading Linux](#) on page 52
- [Stage 2: Loading the primary release](#) on page 52
- [Stage 3: Loading the configuration file](#) on page 52

The following figure shows a summary of the boot sequence.

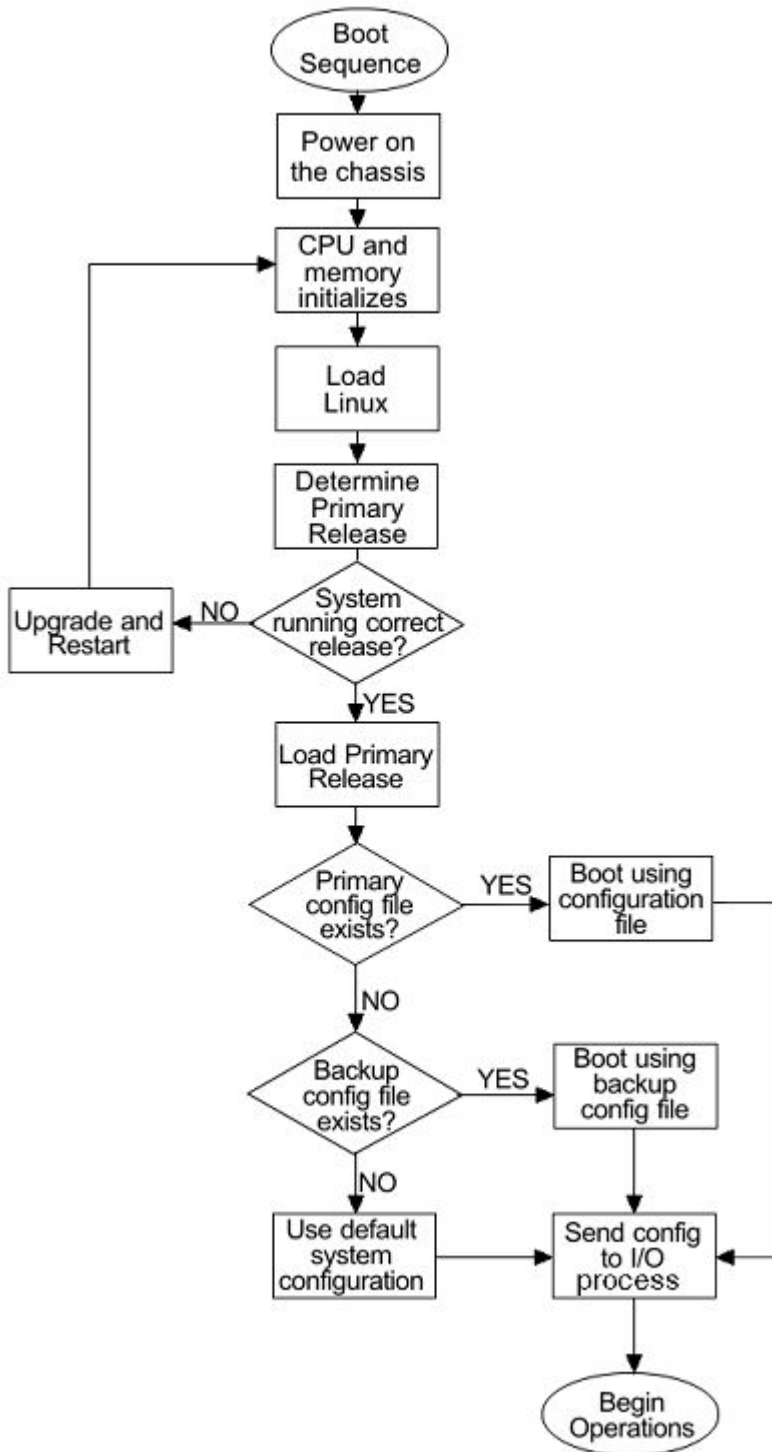


Figure 1: Virtual Services Platform 4000 boot sequence

Stage 1: Loading Linux

The module contains a boot flash partition that stores the boot images, which include the boot loader, and the Linux kernel and applications. The boot flash partition contains two versions of the boot image: a committed version (the primary release) and a backup version. A committed version is one that is marked as good (if you can start the system using that version). The system automatically uses the backup version if the system fails the first time you start with a new version.

Stage 2: Loading the primary release

Virtual Services Platform 4000 can install a maximum of six releases but can only load one of two—a primary (committed) release or a backup release.

The system saves software image files to the `/intflash/release/` directory.

After loading the primary release, the CPU and basic system devices such as the console port initialize. At this stage, the I/O ports are not available; the system does not initialize the I/O ports until the module sends configuration data in stage 3.

Stage 3: Loading the configuration file

The final step before the boot process is complete is to load the configuration data. After the system loads the primary release, it identifies the location and file name of the primary configuration file. You can save this file in internal flash.

If the primary configuration file does not exist, the system looks for the backup configuration file, as identified by `version.cfg`. If this file does not exist, the system loads the factory default configuration.

The switch configuration consists of higher-level functionality, including:

- chassis configuration
- port configuration
- virtual LAN (VLAN) configuration
- routing configuration
- IP address assignments
- remote monitoring (RMON) configuration

The default switch configuration includes the following:

- a single, port-based default VLAN with a VLAN identification number of 1
- no interface assigned IP addresses
- traffic priority for all ports configured to normal priority
- all ports as untagged ports
- default communication protocol settings for the console port. For more information about these protocol settings, see [System connections](#) on page 55.

In the configuration file, statements preceded by both the number sign (#) and exclamation point (!) load prior to the general configuration parameters. Statements preceded by only the number sign are comments meant to add clarity to the configuration; they do not load configuration parameters. The following table illustrates the difference between these two statement formats.

Table 7: Configuration file statements

Sample statement	Action
<code># software version : 4.1.0.0</code>	Adds clarity to the configuration by identifying the software version.
<code>#!no boot config flags sshd</code>	Configures the flag to the false condition, prior to loading the general configuration.

Boot sequence modification

You can change the boot sequence in the following ways:

- Change the primary designations for file sources.
- Change the file names from the default values. You can store several versions of the configuration file and specify a particular one by file name. The specified configuration file only gets loaded when the chassis starts. To load a new configuration file, you need to restart the system.
- Start the system without loading a configuration file, so that the system uses the factory default configuration. Bypassing the system configuration does not affect saved system configuration; the configuration simply does not load. This can be done by setting the factory defaults boot flag.

Run-time

After Virtual Services Platform 4000 is operational, you can use the run-time commands to perform configuration and management functions necessary to manage the system. These functions include the following

- resetting or restarting Virtual Services Platform 4000
- adding, deleting, and displaying address resolution protocol (ARP) table entries
- pinging another network device
- viewing and configuring variables for the entire system and for individual ports
- configuring and displaying MultiLink Trunking (MLT) parameters
- creating and managing port-based VLANs or policy-based VLANs

To access the run-time environment you need a connection from a PC or terminal to the switch. You can use a direct connection to the switch through the console port or remotely through Telnet, rlogin, or Secure Shell (SSH) sessions.

Important:

Before you attempt to access the switch using one of the preceding methods, ensure you first enable the corresponding daemon flags.

Configuration redundancy

You can define primary and backup configuration file paths. This configuration protects against system failures. For example, the primary path can point to system flash memory and the backup path to the external Compact Flash card.

System flags

After you enable or disable certain modes and functions, you need to save the configuration and restart the switch for your change to take effect. This section lists parameters and indicates if they require a switch restart.

The following table lists parameters you configure in ACLI using the `boot config flags` command. For information on system flags and their configuration, see [Configuring system flags](#) on page 64.

Table 8: Boot config flags

ACLI flag	Restart
block-snmp	No
debug-config	Yes
debugmode	Yes
enhancedsecure-mode	Yes
factorydefaults	Yes
ftpd	No
hsecure	Yes
logging	No
reboot	No
rlogind	No
spanning-tree-mode	Yes
sshd	No
telnetd	No
tftpd	No
trace-logging	No
verify-config	Yes
wdt	Yes

System connections

Connect the serial console interface (an RJ45 jack) to a PC or terminal to monitor and configure the switch. The port uses a RJ45 connector that operates as data terminal equipment (DTE). The default communication protocol settings for the console port are:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

To use the console port, you need a terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.

Client and server support

The client-server model partitions tasks between servers that provide a service and clients that request a service.

For active ACLI clients, users initiate a client connection from Virtual Services Platform 4000 to another device.

For non-active clients, the client exists on the switch and the switch console initiates the request, with no intervention from users after the initial setup. For instance, Network Time Protocol (NTP) is a non active client. The switch initiates the client request to the central server to obtain the up-to-date time.

Clients

IPv4 support:

The switch supports the following active ACLI clients using IPv4:

- remote shell (rsh)
- rlogin
- Secure Shell version 2 (SSHv2)
- telnet

The switch supports the following non active client using IPv4:

- Network Time Protocol (NTP)

IPv4 and IPv6 support:

The switch supports the following active ACLI clients using IPv4. and IPv6

- File Transfer Protocol (FTP)
- Telnet client
- Trivial File Transfer Protocol (TFTP)

*** Note:**

FTP and TFTP clients are part of the ACLI `copy` command. You cannot launch FTP and TFTP clients individually. You must use the `copy` command. If you have set the username and password through the `boot config host` command, then FTP is used, otherwise TFTP is used.

Virtual Services Platform 4000 supports the following non active clients using IPv4 and IPv6:

- Domain Name System (DNS)
- Remote Authentication Dial-in User Service (RADIUS)

Servers

IPv4 and IPv6 support:

The switch supports the following servers using IPv4 and IPv6:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- remote shell (rsh)
- rlogin
- Secure Copy (SCP)

*** Note:**

The current release does not support Secure Copy (SCP).

- Secure File Transfer Protocol (SFTP)
- Secure Shell version 2 (SSHv2)
- Telnet
- Trivial File Transfer Protocol (TFTP)

Chapter 6: Boot parameter configuration using ACLI

Use the procedures in this section to configure and manage the boot process.

- To perform the procedures in this section, you must log on to Global Configuration mode in ACLI. For more information about how to use ACLI and how to log on to the software, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.

Related links

[Modifying the boot sequence](#) on page 57

[Configuring the remote host logon](#) on page 58

Modifying the boot sequence

About this task

Modify the boot sequence to prevent the switch from using the factory default settings or, conversely, to prevent loading a saved configuration file.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Bypass the loading of the switch configuration file and load the factory defaults:

```
boot config flags factorydefaults
```

3. Use a configuration file and not the factory defaults:

```
no boot config flags factorydefaults
```

Important:

If the switch fails to read and load a saved configuration file after it starts, please check the log file to see if the log file indicate that the factorydefaults setting was enabled, before you investigate other options.

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
VSP-4850GTS-PWR+:1#boot config flags factorydefaults
```

Related links

[Boot parameter configuration using ACLI](#) on page 57

Configuring the remote host logon

Before you begin

- The FTP server must support the FTP passive (PASV) command. If the FTP server does not support the passive command, the file transfer is aborted, and then the system logs an error message that indicates that the FTP server does not support the passive command.

About this task

Configure the remote host logon to modify parameters for FTP and TFTP access. The defaults allow TFTP transfers. If you want to use FTP as the transfer mechanism, you need to change the password to a non-null value.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Define conditions for the remote host logon:

```
boot config host {ftp-debug|password WORD<0-16>|tftp-debug|tftp-
hash|tftp-rexmit <1-120>|tftp-timeout <1-120>|user WORD<0-16>}
```

3. Save the changed configuration.

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
Enable console tftp/tftpd debug messages:
VSP-4850GTS-PWR+:1#boot config host tftp-debug
VSP-4850GTS-PWR+:1#save config
```

Related links

[Boot parameter configuration using ACLI](#) on page 57

Enabling remote access services

Enable the remote access service to provide multiple methods of remote access.

Before you begin

- If you enable the rlogind flag, you must configure an access policy to specify the name of the user who can access the switch. For more information about access policies, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601.

About this task

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), remote login (rlogin) and Telnet server support IPv4 and IPv6 addresses with no difference in functionality or configuration.

On IPv6 networks, the switch supports SSHv2 server and Remote Shell (rsh) server only. The switch does not support outbound SSHv2 client over IPv6 or rsh client over IPv6. On IPv4 networks, the switch supports both server and client for SSHv2 and rsh.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable the access service:

```
boot config flags {ftpd|rlogind|sshd|telnetd|tftpd}
```

3. Save the configuration.

Example

Enable the access service to SSHv2:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags sshd
```

Variable definitions

Use the data in the following table to use the `boot config flags` command.

Table 9: Variable definitions

Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.
debug-config [console] [file]	Enables you to debug the configuration file during loading configuration at system boot up. The default

Table continues...



Variable	Value
	<p>is disabled. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots.</p> <p>The options are:</p> <ul style="list-style-type: none"> • debug-config [console]—Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file. • debug-config [file]— Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug config output to /intflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to /intflash/debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.
debugmode	<p> Important:</p> <p>Do not change this parameter unless directed by Avaya.</p> <p>Enables debugmode to allow you to enable trace on any module by prompting the selection on the console during boot up. This allows you to start trace to debug earlier on the specified module. It only works on the console connection. By default, it is disabled.</p>
enhancedsecure-mode {jitc non-jitc}	<p>Enables enhanced secure mode in either the JITC or non-JITC sub-modes.</p> <p> Note:</p> <p>The JITC sub-mode is more restrictive and prevents the use of some ACLI commands that are commonly used for troubleshooting. It is recommended that you enable the non-JITC sub-mode.</p> <p>If you enable enhanced secure mode in either the JITC or non-JITC sub-modes, the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change</p>

Table continues...

Variable	Value
	intervals, password reuse, and password maximum age use.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
ftpd	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the tftpd flag is disabled.
hsecure	<p>Activates or disables high secure mode. The hsecure command provides the following password behavior:</p> <ul style="list-style-type: none"> • 10 character enforcement • The password must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 numbers, and 2 special characters. • Aging time • Failed login attempt limitation <p>The default value is disabled. If you enable high secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in high secure mode, the switch prompts a password change if you enter invalid-length passwords.</p>
ipv6-mode	Enables IPv6 mode on the switch.
logging	<p>Activates or disables system logging. The default value is enabled. The system names log files according to the following:</p> <ul style="list-style-type: none"> • The file names appear in 8.3 (log.xxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. • The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file. <p>The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.</p>

Table continues...

Variable	Value
reboot	<p>Activates or disables automatic reboot on a fatal error. The default value is activated.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
rlogind	<p>Activates or disables the rlogin and rsh server. The default value is disabled.</p>
spanning-tree-mode <mstp rstp>	<p>Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.</p>
spbm-config-mode	<p>Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.</p> <p>Use the no operator so that you can configure PIM and IGMP.</p> <p>The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.</p>
sshd	<p>Activates or disables the SSHv2 server service. The default value is disabled.</p>
telnetd	<p>Activates or disables the Telnet server service. The default is disabled.</p>
tftpd	<p>Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.</p>
trace-logging	<p>Activates or disables the creation of trace logs. The default value is disabled.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
verify-config	<p>Activates syntax checking of the configuration file. The default is enabled. Avaya recommends that you disable the verify-config flag.</p> <ul style="list-style-type: none"> • Primary config behavior: When the verifyconfig flag is enabled, the primary config file is pre-checked for syntax errors. If the system finds an error, the primary config file is not loaded, instead the system loads the backup config file.

Table continues...

Variable	Value
	<p>If the verify-config flag is disabled, the system does not pre-check syntax errors. When the verify-config flag is disabled, the system ignores any lines with errors during loading of the primary config file. If the primary config file is not present or cannot be found, the system tries to load the backup file.</p> <ul style="list-style-type: none"> • Backup config behavior: If the system loads the backup config file, the system does not check the backup file for syntax errors. It does not matter if the verify-config flag is disabled or enabled. With the backup config file, the system ignores any lines with errors during the loading of the backup config file. <p>If no backup config file exists, the system defaults to factory defaults.</p>

Changing the primary or secondary boot configuration files

About this task

Change the primary or secondary boot configuration file to specify which configuration file the system uses to start.

Configure the primary boot choices.

You have a primary configuration file that specifies the full directory path and a secondary configuration file that also contains the full directory path.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Change the primary boot choice:

```
boot config primary {backup-config-file|config-file} WORD<0-255>
```

3. Save the changed configuration.
4. Restart the switch.

Example

```
VSP-4850GTS-PWR+:1> enable
```

```
VSP-4850GTS-PWR+:1# configure terminal
```

Specify the configuration file in internal flash memory as the primary boot source:

```
VSP-4850GTS-PWR+:1(config)# boot config primary config-file /intflash/  
config.cfg
```

```
VSP-4850GTS-PWR+:1(config)# save config
```

```
VSP-4850GTS-PWR+:1(config)# reset
```

Variable definitions


Use the data in the following table to use the `boot config` command.

Table 10: Variable definitions

Variable	Value
{backup-config-file config-file}	Specifies that the boot source uses either the configuration file or a backup configuration file.
WORD<0–255>	Identifies the configuration file. <i>WORD<0–255></i> is the device and file name, up to 255 characters including the path, in one of the following format: <ul style="list-style-type: none">• a.b.c.d:<file>• /intflash/<file> To set this option to the default value, use the default operator with the command.

Configuring system flags

Before you begin

- If you enable the `hsecure` flag, you cannot enable the flags for the Web server or SSH password-authentication.
-  **Important:**
After you change certain configuration parameters using the `boot config flags` command, you must save the changes to the configuration file.

About this task

Configure the system flags to enable specific services and functions for the chassis.

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) and Telnet server support IPv4 and IPv6 addresses, with no difference in functionality or configuration.

On IPv6 networks, VSP 4000 supports SSH server, remote login (rlogin) server and Remote Shell (rsh) server only. VSP 4000 does not support outbound SSH client over IPv6, rlogin client over IPv6

or rsh client over IPv6. On IPv4 networks, VSP 4000 supports both server and client for SSH, rlogin and rsh.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable system flags:

```
boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode <jitc|non-jitc> |factorydefaults|ftpd|hsecure|
logging|reboot|rlogind|spbm-config-mode|spanning-tree-mode <mstp|
rstp>|sshd|telnetd|tftpd|trace-logging|verify-config>
```

3. Disable system flags:

```
no boot config flags <block-snmp|debug-config|debugmode|
enhancedsecure-mode|factorydefaults|ftpd|hsecure|logging|reboot|
rlogind|spbm-config-mode|spanning-tree-mode|sshd|telnetd|tftpd|
trace-logging|verify-config>
```

4. Configure the system flag to the default value:

```
default boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode|factorydefaults|ftpd|hsecure|logging|reboot|
rlogind|spbm-config-mode|spanning-tree-mode|sshd|telnetd|tftpd|
trace-logging|verify-config>
```

5. Save the changed configuration.

6. Restart the switch.

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
Activate High Secure mode:
VSP-4850GTS-PWR+:1(config)#boot config flags hsecure
VSP-4850GTS-PWR+:1(config)#save config
VSP-4850GTS-PWR+:1(config)#reset
```

Variable definitions

Use the data in the following table to use the `boot config flags` command.

Table 11: Variable definitions



Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.
debug-config [console] [file]	<p>Enables you to debug the configuration file during loading configuration at system boot up. The default is disabled. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots.</p> <p>The options are:</p> <ul style="list-style-type: none"> • debug-config [console]—Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file. • debug-config [file]— Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug config output to /intflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to /intflash/debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.
debugmode	<p> Important:</p> <p>Do not change this parameter unless directed by Avaya.</p> <p>Enables debugmode to allow you to enable trace on any module by prompting the selection on the console during boot up. This allows you to start trace to debug earlier on the specified module. It only works on the console connection. By default, it is disabled.</p>
enhancedsecure-mode {jitc non-jitc}	<p>Enables enhanced secure mode in either the JITC or non-JITC sub-modes.</p> <p> Note:</p> <p>The JITC sub-mode is more restrictive and prevents the use of some ACLI commands that are commonly used for troubleshooting. It is recommended that you enable the non-JITC sub-mode.</p>

Table continues...

Variable	Value
	If you enable enhanced secure mode in either the JITC or non-JITC sub-modes, the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
ftpd	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the tftpd flag is disabled.
hsecure	<p>Activates or disables high secure mode. The hsecure command provides the following password behavior:</p> <ul style="list-style-type: none"> • 10 character enforcement • The password must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 numbers, and 2 special characters. • Aging time • Failed login attempt limitation <p>The default value is disabled. If you enable high secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in high secure mode, the switch prompts a password change if you enter invalid-length passwords.</p>
ipv6-mode	Enables IPv6 mode on the switch.
logging	<p>Activates or disables system logging. The default value is enabled. The system names log files according to the following:</p> <ul style="list-style-type: none"> • The file names appear in 8.3 (log.xxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. • The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file.

Table continues...

Variable	Value
	The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
reboot	<p>Activates or disables automatic reboot on a fatal error. The default value is activated.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
spanning-tree-mode <mstp rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
spbm-config-mode	<p>Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.</p> <p>Use the no operator so that you can configure PIM and IGMP.</p> <p>The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.</p>
sshd	Activates or disables the SSHv2 server service. The default value is disabled.
telnetd	Activates or disables the Telnet server service. The default is disabled.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
trace-logging	<p>Activates or disables the creation of trace logs. The default value is disabled.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
verify-config	<p>Activates syntax checking of the configuration file. The default is enabled. Avaya recommends that you disable the verify-config flag.</p> <ul style="list-style-type: none"> • Primary config behavior: When the verifyconfig flag is enabled, the primary config file is pre-checked for syntax errors. If the system finds an error, the

Table continues...

Variable	Value
	<p>primary config file is not loaded, instead the system loads the backup config file.</p> <p>If the verify-config flag is disabled, the system does not pre-check syntax errors. When the verify-config flag is disabled, the system ignores any lines with errors during loading of the primary config file. If the primary config file is not present or cannot be found, the system tries to load the backup file.</p> <ul style="list-style-type: none"> • Backup config behavior: If the system loads the backup config file, the system does not check the backup file for syntax errors. It does not matter if the verify-config flag is disabled or enabled. With the backup config file, the system ignores any lines with errors during the loading of the backup config file. <p>If no backup config file exists, the system defaults to factory defaults.</p>

Configuring serial port devices

About this task

Configure the serial port devices to define connection settings for the console port .

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Optionally, specify 8 data bits:


```
boot config sio console 8databits
```
3. Optionally, change the baud rate for the port:


```
boot config sio console baud <9600-115200>
```
4. Save the changed configuration.
5. Restart the switch.

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#config terminal
```

Configure the baud rate to 9600 for the port:

```
VSP-4850GTS-PWR+:1(config)#boot config sio console baud 9600
```

Variable definitions

Use the data in the following table to use the `boot config sio console` command.

Table 12: Variable definitions

Variable	Value
8databits	Specifies either 8 (true) or 7 (false) data bits for each byte for the software to interpret. The default value is 8 data bits. Use the <code>no</code> or default operator with the command to configure this variable to the false condition.
baud <9600–115200>	Configures the baud rate for the port from one of: <ul style="list-style-type: none">• 9600• 19200• 38400• 57600• 115200 The default value is 9600. To configure this option to the default value, use the default operator with the command.

Displaying the boot configuration

About this task

Display the configuration to view current or changed settings for the boot parameters.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. View the configuration:

```
show boot config <choice|flags|general|host|running-config  
[verbose]|sio>
```

Example

Show the current boot configuration. (If you omit `verbose`, the system only displays the values that you changed from their default value.):

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

VSP-4850GTS-PWR+:1#(config)#show boot config running-config
#
#Tue Feb 19 15:12:01 2012 UTC
#
boot config flags ftpd
boot config flags rlogind
boot config flags sshd
boot config flags telnetd
boot config flags tftpd
no boot config flags verify-config
boot config choice primary backup-config-file "/intflash/config.cfg"
```

Variable definitions

Use the data in the following table to use the `show boot config` command.

Table 13: Variable definitions

Variable	Value
choice	Shows the current boot configuration choices.
flags	Shows the current flag settings.
general	Shows system information.
host	Shows the current host configuration.
running-config [verbose]	Shows the current boot configuration. If you use verbose, the system displays all possible information. If you omit verbose, the system displays only the values that you changed from their default value.
sio	Specifies the current configuration of the serial ports.

Chapter 7: Run-time process management using ACLI

Configure and manage the run-time process using the Avaya Command Line Interface (ACLI).

To perform the procedures in this section, you must log on to Global Configuration mode in ACLI. For more information about how to use ACLI, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.

Related links

[Configuring the time zone](#) on page 73

Configuring the date

Before you begin

- You must log on as rwa to perform this procedure.

About this task

Configure the calendar time in the form of month, day, year, hour, minute, and second.

Procedure

1. Enter the Privileged EXEC mode:
`enable`
2. Configure the date:
`clock set <MMddyyyyhhmmss>`

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#clock set 11062011063030
```

Variable definitions

Use the data in the following table to use the `clock set` command.

Table 14: Variable definitions

Variable	Value
MMddyyyyhhmmss	Specifies the date and time in the format month, day, year, hour, minute, and second.

Configuring the time zone

About this task

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data in Linux includes daylight changes for all time zones up to the year 2038. You do not need to configure daylight savings.

The default time zone is Coordinated Universal Time (UTC).

Important:

According to a recent bill passed by the government of Russia, from October 2014, Moscow has moved from current UTC+4 into UTC+3 time zone, with no daylight savings.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure the time zone by using the following command:

```
clock time-zone WORD<1-10> WORD<1-20> WORD<1-20>
```

3. Save the changed configuration.

Example

Configure the system to use the time zone data file for Vevay:

```
Switch:1(config)# clock time-zone America Indiana Vevay
```

Related links

[Run-time process management using ACLI](#) on page 72

[Variable definitions](#) on page 73

Variable definitions

Use the data in the following table to use the `clock time-zone` command.

Table 15: Variable definitions

Variable	Value
<i>WORD</i> <1–10>	Specifies a directory name or a time zone name in /usr/share/zoneinfo, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter <code>clock time-zone</code> at the command prompt without variables.
<i>WORD</i> <1–20> <i>WORD</i> <1–20>	The first instance of <i>WORD</i> <1–20> is the area within the timezone. The value represents a time zone data file in /usr/share/zoneinfo/ <i>WORD</i> <1–10>/, for example, Shanghai in Asia. The second instance of <i>WORD</i> <1–20> is the subarea. The value represents a time zone data file in /usr/share/zoneinfo/ <i>WORD</i> <1–10>/ <i>WORD</i> <1–20>/, for example, Vevay in America/Indiana. To see a list of options, enter <code>clock time-zone</code> at the command prompt without variables.

Related links

[Configuring the time zone](#) on page 73

Configuring the run-time environment

About this task

Configure the run-time environment to define generic configuration settings for ACLI sessions.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Change the login prompt:


```
login-message WORD<1-1513>
```
3. Change the password prompt:


```
passwordprompt WORD<1-1510>
```
4. Configure the number of supported rlogin sessions:


```
max-logins <0-8>
```
5. Configure the number of supported inbound Telnet sessions:


```
telnet-access sessions <0-8>
```
6. Configure the idle timeout period before automatic logoff for ACLI and Telnet sessions:


```
cli timeout <30-65535>
```

7. Configure the number of lines in the output display:

```
terminal length <8-64>
```

8. Configure scrolling for the output display:

```
terminal more <disable|enable>
```

*** Note:**

`terminal more disable` does not shut off screen output paging when you use the `show fulltech` command from the serial console port; it does shut off screen output paging for all other commands.

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:#configure terminal
```

Use the default option to enable use of the default logon string:

```
VSP-4850GTS-PWR+: (config)#default login-message
```

Use the default option before this parameter to enable use of the default string:

```
VSP-4850GTS-PWR+: (config)#default passwordprompt
```

Configure the allowable number of inbound remote ACLI logon sessions:

```
VSP-4850GTS-PWR+: (config)#max-logins 5
```

Configure the allowable number of inbound Telnet sessions:

```
VSP-4850GTS-PWR+: (config)#telnet-access sessions 8
```

Configure the timeout value, in seconds, to wait for a Telnet or ACLI login session before terminating the connection:

```
VSP-4850GTS-PWR+: (config)#cli timeout 900
```

Configure the number of lines in the output display for the current session:

```
VSP-4850GTS-PWR+: (config)#terminal length 30
```

Configure scrolling for the output display:

```
VSP-4850GTS-PWR+: (config)#terminal more disable
```

Variable definitions

Use the data in the following table to use the `login-message` command.

Table 16: Variable definitions

Variable	Value
<i>WORD</i> <1-1513>	<p>Changes the ACLI logon prompt.</p> <ul style="list-style-type: none"> • <i>WORD</i><1-1513> is an American Standard Code for Information Interchange (ASCII) string from 1–1513 characters. • Use the default option before this parameter, <code>default login-message</code>, to enable use of the default logon string. • Use the no operator before this parameter, <code>no login-message</code>, to disable the default logon banner and display the new banner.

Use the data in the following table to use the `passwordprompt` command.

Table 17: Variable definitions

Variable	Value
<i>WORD</i> <1-1510>	<p>Changes the ACLI password prompt.</p> <ul style="list-style-type: none"> • <i>WORD</i><1-1510> is an ASCII string from 1–1510 characters. • Use the default option before this parameter, <code>default passwordprompt</code>, to enable using the default string. • Use the no operator before this parameter, <code>no passwordprompt</code>, to disable the default string.

Use the data in the following table to use the `max-logins` command.

Table 18: Variable definitions

Variable	Value
<0-8>	Configures the allowable number of inbound remote ACLI logon sessions. The default value is 8.

Use the data in the following table to use the `telnet-access sessions` command.

Table 19: Variable definitions

Variable	Value
<0-8>	Configures the allowable number of inbound Telnet sessions. The default value is 8.

Use the data in the following table to use the `cli time-out` command.

Table 20: Variable definitions

Variable	Value
<30-65535>	Configures the timeout value, in seconds, to wait for a Telnet or ACLI login session before terminating the connection.

Use the data in the following table to use the `terminal` command.

Table 21: Variable definitions

Variable	Value
<8-64>	Configures the number of lines in the output display for the current session. To configure this option to the default value, use the <code>default</code> operator with the command. The default is value 23.
disable enable	Configures scrolling for the output display. The default is enabled. Use the <code>no</code> operator to remove this configuration. To configure this option to the default value, use the default operator with the command. no

Configuring the logon banner

About this task

Configure the logon banner to display a warning message to users before authentication.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the switch to use a custom banner or use the default banner:

```
banner <custom|static>
```

3. Create a custom banner:

```
banner WORD<1-80>
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
```

Activate the use of the default banner:

```
VSP-4850GTS-PWR+:1(config)#banner static
```

Variable definitions

Use the data in the following table to use the `banner` command.

Table 22: Variable definitions

Variable	Value
custom static	Activates or disables use of the default banner.
displaymotd	Enables displaymotd.
motd	Sets the message of the day banner.
WORD<1–80>	Adds lines of text to the ACLI logon banner.

Configuring the message-of-the-day

About this task

Configure a system login message-of-the-day in the form of a text banner that appears after each successful logon.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. Create the message-of-the-day:

```
banner motd WORD<1-1516>
```
3. Enable the custom message-of-the-day:

```
banner displaymotd
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Create a message-of-the-day to display with the logon banner. (To provide a string with spaces, include the text in quotation marks.):

```
VSP-4850GTS-PWR+:1(config)#banner motd "Unauthorized access is forbidden"
```

Enable the custom message-of-the-day:

```
VSP-4850GTS-PWR+:1(config)#banner displaymotd
```

Variable definitions

Use the data in the following table to use the `banner motd` command.

Table 23: Variable definitions

Variable	Value
<code>WORD<1-1516></code>	Creates a message of the day to display with the logon banner. To provide a string with spaces, include the text in quotation marks ("). To set this option to the default value, use the default operator with the command.

Configuring ACLI logging

Use ACLI logging to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as CLILog module.

About this task

*** Note:**

The platform logs CLILog and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILog and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Enable ACLI logging:


```
clilog enable
```
3. **(Optional)** Disable ACLI logging:


```
no clilog enable
```
4. Ensure that the configuration is correct:


```
show clilog
```
5. View the ACLI log:


```
show logging file module clilog
```

Example

Enable ACLI logging, and view the ACLI log:

```

Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#clilog enable
Switch:1(config)#show logging file module clilog
CP1 [02/13/13 17:27:25.956] 0x002c0600 00000000 GlobalRouter CLILOG INFO 1 CONSOLE
rwa show snmp-server host
CP1 [02/13/13 17:28:10.100] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2 CONSOLE
rwa show snmp-server notif
CP1 [02/13/13 17:28:45.732] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3 CONSOLE
rwa snmp-server force-trap
CP1 [02/13/13 17:29:30.628] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4 CONSOLE
rwa show logging file modug
CP1 [02/14/13 19:39:11.648] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5 CONSOLE
rwa ena
CP1 [02/14/13 19:39:13.420] 0x002c0600 00000000 GlobalRouter CLILOG INFO 6 CONSOLE
rwa conf t
CP1 [02/14/13 19:49:21.044] 0x002c0600 00000000 GlobalRouter CLILOG INFO 7 CONSOLE
rwa filter acl 2 enable
CP1 [02/14/13 19:50:08.540] 0x002c0600 00000000 GlobalRouter CLILOG INFO 8 CONSOLE
rwa filter acl 2 type inpol
CP1 [02/14/13 19:50:38.444] 0x002c0600 00000000 GlobalRouter CLILOG INFO 9 CONSOLE
rwa filter acl 2 type inpoe
CP1 [02/14/13 19:50:52.968] 0x002c0600 00000000 GlobalRouter CLILOG INFO 10 CONSOLE
rwa filter acl enable 2
CP1 [02/14/13 19:51:08.908] 0x002c0600 00000000 GlobalRouter CLILOG INFO 11 CONSOLE
rwa filter acl 2 enable
CP1 [02/15/13 06:50:25.972] 0x002c0600 00000000 GlobalRouter CLILOG INFO 14 CONSOLE
rwa ena
CP1 [02/15/13 06:50:30.288] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15 CONSOLE
rwa conf t
CP1 [02/15/13 06:50:39.412] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16 CONSOLE
rwa show vlan basic
CP1 [02/15/13 06:51:09.488] 0x002c0600 00000000 GlobalRouter CLILOG INFO 17 CONSOLE
rwa show isis spbm
CP1 [02/15/13 06:56:00.992] 0x002c0600 00000000 GlobalRouter CLILOG INFO 19 CONSOLE
rwa spbm 23 b-vid 2 primar1
CP1 [02/15/13 06:56:59.092] 0x002c0600 00000000 GlobalRouter CLILOG INFO 20 CONSOLE
rwa show isis
CP1 [02/15/13 07:10:54.928] 0x002c0600 00000000 GlobalRouter CLILOG INFO 21 CONSOLE
rwa show isis interface
CP1 [02/15/13 07:12:33.404] 0x002c0600 00000000 GlobalRouter CLILOG INFO 22 CONSOLE
rwa show isis spbm
CP1 [02/15/13 07:45:28.596] 0x002c0600 00000000 GlobalRouter CLILOG INFO 23 CONSOLE
rwa ena
CP1 [02/15/13 07:45:30.236] 0x002c0600 00000000 GlobalRouter CLILOG INFO 24 CONSOLE
rwa conf t
CP1 [02/15/13 07:46:29.456] 0x002c0600 00000000 GlobalRouter CLILOG INFO 25 CONSOLE
rwa interface gigabitEther0
CP1 [02/15/13 07:47:28.476] 0x002c0600 00000000 GlobalRouter CLILOG INFO 26 CONSOLE
rwa encapsulation dot1q

--More-- (q = quit)

```

Variable definitionsUse the data in the following table to use the `clilog` commands.

Table 24: Variable definitions

Variable	Value
enable	Activates ACLI logging. To disable, use the <code>no cli log enable</code> command.

Configuring system parameters

About this task

Configure individual system-level switch parameters to configure global options for Avaya Virtual Services Platform 4000 Series.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Change the system name:

```
sys name WORD<0-255>
```

3. Enable support for Jumbo frames:

```
sys mtu 1950
```

OR

```
sys mtu 9600
```

4. Enable the User Datagram Protocol (UDP) checksum calculation:

```
udp checksum
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Configure the system, or root level, prompt name for the switch:

```
VSP-4850GTS-PWR+:1(config)#sys name Floor3Lab2
```

Variable definitions

Use the data in the following table to use the `sys` command.

Table 25: Variable definitions

Variable	Value
mtu <1522 9600>	Activates Jumbo frame support for the data path. The value can be either 1522, 1950 (default), or 9600 bytes. 1950 or 9600 bytes activate Jumbo frame support.
name <i>WORD</i> <0–255>	Configures the system, or root level, prompt name for the switch. <i>WORD</i> <0–255> is an ASCII string from 0–255 characters (for example, LabSC7 or Closet4).
clipld-topology-ip	Set the topology ip from the available CLIP. <i>WORD</i> <1-256> Circles the ip interface id.
force-msg	Adds forced message control pattern. <i>WORD</i> <4–4> Enter force message pattern.
force-topology-ip-flag	Flag set to force choice of topology flag. <i>enable</i>
msg-control	Enables system message control feature.

Configuring system message control

About this task

Configure system message control to suppress duplicate error messages on the console, and to determine the action to take if they occur.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Configure system message control action:


```
sys msg-control action <both|send-trap|suppress-msg>
```
3. Configure the maximum number of messages:


```
sys msg-control max-msg-num <2-500>
```
4. Configure the interval:


```
sys msg-control control-interval <1-30>
```
5. Enable message control:


```
sys msg-control
```


Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Configure system message control to suppress duplicate error messages on the console and send a trap notification:

```
VSP-4850GTS-PWR+:1(config)#sys msg-control action both
```

Configure the number of occurrences of a message after which the control action occurs:

```
VSP-4850GTS-PWR+:1(config)#sys msg-control max-msg-num 2
```

Configure the message control interval in minutes:

```
VSP-4850GTS-PWR+:1(config)#sys msg-control control-interval 3
```

Enable message control:

```
VSP-4850GTS-PWR+:1(config)#sys msg-control
```

Variable definitions

Use the data in the following table to use the `sys msg-control` command.

Table 26: Variable definitions

Variable	Value
action <both send-trap suppress-msg>	Configures the message control action. You can either suppress the message or send a trap notification, or both. The default is suppress.
control-interval <1-30>	Configures the message control interval in minutes. The valid options are 1–30. The default is 5.
max-msg-num <2-500>	Configures the number of occurrences of a message after which the control action occurs. To configure the maximum number of occurrences, enter a value from 2–500. The default is 5.

Extending system message control**About this task**

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. Configure the force message control option:

```
sys force-msg WORD<4-4>
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Configure the force message control option. (If you specify the wildcard pattern (****), then all messages undergo message control:

```
VSP-4850GTS-PWR+:1(config)#sys force-msg ****
```

Variable definitions

Use the data in the following table to use the `sys force-msg` command.

Table 27: Variable definitions

Variable	Value
<i>WORD<4-4></i>	Adds a forced message control pattern, where <i>WORD<4-4></i> is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes that match one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****) as well. If you specify the wildcard pattern, all messages undergo message control.

Chapter 8: Chassis operations fundamentals

This section provides conceptual information for chassis operations such as hardware and software compatibility and power management. Read this section before you configure the chassis operations.

Software lock-up detection

The software lock-up detect feature monitors processes on the CPU to limit situations where the device stops functioning because of a software process issue. Monitored issues include

- software that enters a dead-lock state
- a software process that enters an infinite loop

The software lock-up detect feature monitors processes to ensure that the software functions within expected time limit.

The CPU logs detail about suspended tasks in the log file. For additional information about log files, see *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702.

Jumbo frames

Jumbo packets and large packets are particularly useful in server and storage over Ethernet applications. If the payload to header relation increases in a packet, the bandwidth can be used more efficiently. For this reason, increasing Ethernet frame size is a logical option. Avaya Virtual Services Platform 4000 Series supports Ethernet frames as large as 9600 bytes, compared to the standard 1518 bytes, to transmit large amounts of data efficiently and minimize the task load on a server CPU.

Tagged VLAN support

A port with VLAN tagging activated can send tagged frames. If you plan to use Jumbo frames in a VLAN, ensure that you configure the ports in the VLAN to accept Jumbo frames and that the server or hosts in the VLAN do not send frames that exceed 9600 bytes. For more information about how to configure VLANs, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500.

SynOptics Network Management Protocol

Avaya Virtual Services Platform 4000 Series ports support an auto-discovery protocol known as the SynOptics Network Management Protocol (SONMP). SONMP allows a network management station (NMS) to formulate a map that shows the interconnections between Layer 2 devices in a network. SONMP is also called Topology Discovery Protocol (TDP).

All devices in a network that are SONMP-enabled send hello packets to their immediate neighbors, that is, to interconnecting Layer 2 devices. A hello packet advertises the existence of the sending device and provides basic information about the device, such as the IP address and MAC address. The hello packets allow each device to construct a topology table of its immediate neighbors. A network management station periodically polls devices in its network for these topology tables, and then uses the data to formulate a topology map.

If you disable SONMP, the system stops transmitting and acknowledging SONMP hello packets. In addition, the system removes all entries in the topology table except its own entry. If you enable SONMP, the system transmits a hello packet every 12 seconds. The default status is enabled.

10/100/1000BASE-TX Auto-Negotiation recommendations

Auto-Negotiation lets devices share a link and automatically configures both devices so that they take maximum advantage of their abilities. Auto-Negotiation uses a modified 10BASE-T link integrity test pulse sequence to determine device ability.

The Auto-Negotiation feature allows the devices to switch between the various operational modes in an ordered fashion and allows management to select a specific operational mode. The Auto-Negotiation feature also provides a parallel detection (also called autosensing) function to allow the recognition of 10BASE-T, 100BASE-TX, 100BASE-T4, and 1000BASE-TX compatible devices, even if they do not support Auto-Negotiation. In this case, only the link speed is sensed; not the duplex mode.

Avaya recommends the Auto-Negotiation configuration as shown in the following table, where A and B are two Ethernet devices.

Table 28: Recommended Auto-Negotiation configuration on 10/100/1000BASE-TX ports

Port on A	Port on B	Remarks	Recommendations
Auto-Negotiation enabled	Auto-Negotiation enabled	Ports negotiate on highest supported mode on both sides.	Avaya recommends that you use this configuration if both ports support Auto-Negotiation mode.
Full-duplex	Full-duplex	Both sides require the same mode.	Avaya recommends that you use this configuration if you require full-duplex, but the configuration does not support Auto-Negotiation.

Auto-Negotiation cannot detect the identities of neighbors or shut down misconnected ports. Upper-layer protocols perform these functions.

*** Note:**

The 10 GigabitEthernet fiber-based I/O module ports can operate at either 1 Gigabit per second (Gbps) or 10 Gbps, depending upon the capabilities of the optical transceiver that you install.

This presents an ambiguity with respect to the auto-negotiation settings of the port, while 1 Gigabit Ethernet (GbE) ports require auto-negotiation; auto-negotiation is not defined and is non-existent for 10 GbE ports.

For a 10GbE fiber-based I/O module, you have the capability to swap back-and-forth between 1 GbE and 10 GbE operation by simply swapping transceivers. To help with this transition between 1 GbE and 10 GbE port operation, Avaya allows you to configure auto-negotiation when you install a 10 GbE transceiver, even though auto-negotiation is not defined for 10GbE.

You can do this in anticipation of a port changeover from 10 GbE to 1 GbE. In this manner, you can essentially pre-configure a port in 1 GbE mode while the 10 GbE transceiver is still installed. The port is ready to go upon the changeover to the 1 GbE transceiver.

In addition, you can use a saved configuration file with auto-negotiation enabled, to boot a system with either 10 GbE or 1 GbE transceivers installed. If you install a 1 GbE transceiver, the system applies auto-negotiation. If you install a 10 GbE transceiver, the system does not remove the auto-negotiation settings from the configuration, but the system simply ignores the configuration because auto-negotiation settings are irrelevant to a 10 GbE transceiver. The system preserves the saved configuration for auto-negotiation when re-saved no matter which speed of transceiver you install.

CANA

Use Custom Auto-Negotiation Advertisement (CANA) to control the speed and duplex settings that the interface modules advertise during Auto-Negotiation sessions between Ethernet devices. Modules can only establish links using these advertised settings, rather than at the highest common supported operating mode and data rate.

Use CANA to provide smooth migration from 10/100 Mbps to 1000 Mbps on host and server connections. Using Auto-Negotiation only, the switch always uses the fastest possible data rates. In limited-uplink-bandwidth scenarios, CANA provides control over negotiated access speeds, and improves control over traffic load patterns.

You can use CANA only on fixed RJ-45 Ethernet ports. To use CANA, you must enable Auto-Negotiation.

! Important:

If a port belongs to a MultiLink Trunking (MLT) group and you configure CANA on the port (that is, you configure an advertisement other than the default), you must apply the same configuration to all other ports of the MLT group (if they support CANA).

Auto MDIX

Automatic medium-dependent interface crossover (Auto-MDIX) automatically detects the need for a straight-through or crossover cable connection and configures the connection appropriately. This removes the need for crossover cables to interconnect switches and ensures either type of cable can be used. The speed and duplex setting of an interface must be set to Auto for Auto-MDIX to operate correctly.

Auto MDIX is supported on all platforms with fixed copper ports. All fixed copper ports are supported.

Chapter 9: Chassis operations configuration using ACLI

This section provides the details to configure basic hardware and system settings.

Related links

[Configuring SONMP](#) on page 91

[Associating a port to a VRF instance](#) on page 93

[Configuring Ethernet ports with Autonegotiation](#) on page 94

[Enabling or disabling the USB port](#) on page 97

Enabling jumbo frames

About this task

Enable jumbo frames to increase the size of Ethernet frames the chassis supports.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable jumbo frames:

```
sys mtu <1950|1522|9600>
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
Enable jumbo frames to 9600 bytes:
VSP-4850GTS-PWR+:1#(config)#sys mtu 9600
```

Variable definitions

Use the data in the following table to use the `sys mtu` command.

Table 29: Variable definitions

Variable	Value
1950 9600	Configures the frame size support for the data path. <1950 9600> is the Ethernet frame size. Possible sizes are 1522, 1950 (default), or 9600 bytes. A configuration of either 1950 or 9600 bytes activates jumbo frame support.

Configuring port lock

About this task

Configure port lock to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify a locked port until you unlock the port.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Enable port lock globally:


```
portlock enable
```
3. Log on to GigabitEthernet Interface Configuration mode:


```
interface gigabitethernet {slot/port[-slot/port][,...]}
```
4. Lock a port:


```
lock port {slot/port[-slot/port][,...]} enable
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
Log on to GigabitEthernet Interface Configuration mode:
VSP-4850GTS-PWR+:1(config)#interface GigabitEthernet 1/1
Unlock port 1/14:
```



```
VSP-4850GTS-PWR+:1(config-if)#no lock port 1/14 enable
```

Variable definitions

Use the data in the following table to use the `interface gigabitethernet` command.

Table 30: Variable definitions

Variable	Value
{slot/port[-slot/port][,...]}	Specifies the port you want to configure.

Use the data in the following table to use the `lock port` command.

Table 31: Variable definitions

Variable	Value
{slot/port[-slot/port][,...]}	Specifies the port you want to lock. Use the <code>no</code> form of this command to unlock a port: <code>no lock port {slot/port[-slot/port][,...]}</code>

Configuring SONMP

About this task

Configure the SynOptics Network Management Protocol (SONMP) to allow a network management station (NMS) to formulate a map that shows the interconnections between Layer 2 devices in a network. The default status is enabled.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable SONMP:

```
no autotopology
```

3. Enable SONMP:

```
autotopology
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1configure terminal
```

Disable SONMP:

```
VSP-4850GTS-PWR+:1 (config)#no autotopology
```

Related links

[Chassis operations configuration using ACLI](#) on page 89

Viewing the topology message status

About this task

View topology message status to view the interconnections between Layer 2 devices in a network.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Show the contents of the topology table:

```
show autotopology nmm-table
```

Unless the VSP 4000 is physically connected to other devices in the network, this topology will be blank.

Example

```
VSP-4850GTS-PWR+:1>show autotopology nmm-table
```

```
=====
                                     Topology Table
=====
Local                               Rem
Port IpAddress      SegmentId MacAddress  ChassisType  BT  LS  CS  Port
-----
```

Job aid

The following table describes the column headings in the command output for `show autotopology nmm-table`.

Table 32: Variable definitions

Variable	Value
Local Port	Specifies the slot and port that received the topology message.
IpAddress	Specifies the IP address of the sender of the topology message.
SegmentId	Specifies the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.

Table continues...

Variable	Value
MacAddress	Specifies the MAC address of the sender of the topology message.
ChassisType	Specifies the chassis type of the device that sent the topology message.
BT	Specifies the backplane type of the device that sent the topology message. Avaya Virtual Services Platform 4000 Series uses a backplane type of 12.
LS	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CS	Specifies the current state of the sender of the topology message. The choices are <ul style="list-style-type: none"> • topChanged—Topology information recently changed. • HtBt (heartbeat)—Topology information is unchanged. • new—The sending agent is in a new state.
Rem Port	Specifies the slot and port that sent the topology message.

Associating a port to a VRF instance

Associate a port to a Virtual Router Forwarding (VRF) instance so that the port becomes a member of the VRF instance.

Before you begin

- The VRF instance must exist. For more information about the creation of VRFs, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505.

About this task

You can assign a VRF instance to a port after you configure the VRF. The system assigns ports to the Global Router, VRF 0, by default.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interfaceGigabitEthernet {slot/port[-slot/port][, ...]} OR interface
vlan <1-4084>
```

2. Associate a VRF instance with a port:

```
vrf <WORD 0-16>
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
```

```
VSP-4850GTS-PWR+:1#interface gigabitethernet 1/12
VSP-4850GTS-PWR+:1#vrf red
```

Related links

[Chassis operations configuration using ACLI](#) on page 89

Configuring Ethernet ports with Autonegotiation

Configure Ethernet ports so they operate optimally for your network conditions. These ports use the Small Form Factor Pluggable plus (SFP+) transceivers. The default is enabled.

About this task

! Important:

- Avaya recommends that all ports that belong to the same MLT or Link Aggregation Control Protocol (LACP) group use the same port speed. In the case of MLTs, the software does not enforce this.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

```
enable
configure terminal
interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-
port]][,...]}
```

* Note:

If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable Autonegotiation:

```
auto-negotiate [port {slot/port[-slot/port][,...]}] enable
```

3. Disable Autonegotiation:

```
no auto-negotiate [port {slot/port[-slot/port][,...]}] enable
```

Example

```
Switch:>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitethernet 4/2
Switch:1(config-if)#auto-negotiate enable
```

Variable definitions

Use the data in following table to use the `auto-negotiate` command.

Variable	Value
port {slot/port[-slot/port][,...]}	Specifies the port or ports that you want to configure.
enable]	<p>Enables Autonegotiation for the port or other ports of the module.</p> <p>The default form of this command is <code>default auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]</code>.</p> <p>The no form of this command is <code>no auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]</code>.</p> <p>* Note:</p> <p>The 10 GigabitEthernet fiber-based I/O module ports can operate at either 1 Gigabit per second (Gbps) or 10 Gbps, dependent upon the capabilities of the optical transceiver that you install.</p> <p>This presents an ambiguity with respect to the autonegotiation settings of the port, while 1 Gigabit Ethernet (GbE) ports require autonegotiation; autonegotiation is not defined and is non-existent for 10 GbE ports.</p> <p>For a 10GbE fiber-based I/O module, you have the capability to swap back-and-forth between 1 GbE and 10 GbE operation by simply swapping transceivers. To help with this transition between 1 GbE and 10 GbE port operation, Avaya allows you to configure autonegotiation when you install a 10 GbE transceiver, even though autonegotiation is not defined for 10GbE.</p> <p>You can do this in anticipation of a port changeover from 10 GbE to 1 GbE. In this manner, you could essentially preconfigure a port in 1 GbE mode while the 10 GbE transceiver is still installed. The port is ready to go upon the changeover to the 1 GbE transceiver.</p> <p>In addition, you can use a saved configuration file with autonegotiation enabled to boot a</p>

Table continues...

Variable	Value
	<p>system with either 10 GbE or 1 GbE transceivers installed. If you install a 1 GbE transceiver, the system applies autonegotiation. If you install a 10 GbE transceiver, the system does not remove the autonegotiation settings from the configuration, but the system simply ignores the configuration because autonegotiation settings are irrelevant to a 10 GbE transceiver. The system preserves the saved configuration for autonegotiation when resaved no matter which speed of transceiver you install.</p>

Configuring serial management port dropping

Configure the serial management ports to drop a connection that is interrupted for any reason. If you enable serial port dropping, the serial management ports drop the connection for the following reasons:

- modem power failure
- link disconnection
- loss of the carrier

Serial ports interrupted due to link disconnection, power failure, or other reasons force out the user and end the user session. Ending the user session ensures a maintenance port is not available with an active session that can allow unauthorized use by someone other than the authenticated user, and prevents the physical hijacking of an active session by unplugging the connected cable and plugging in another.

By default, the feature is disabled with enhanced secure mode disabled. If enhanced secure mode is enabled, the default is enabled.

For more information on enhanced secure mode, see [Enabling enhanced secure mode](#) on page 225.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the serial port to drop if a connection is interrupted:

```
sys security-console
```

Example

Configure the serial port to drop if a connection is interrupted:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#sys security-console
```

Enabling or disabling the USB port

Perform this procedure to control USB access. For security reasons, you may want to disable this port to prevent individuals from using it. By default, the port is automatically mounted when a USB device is inserted.

Important:

Do not perform this procedure on a VSP 4850.

The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

Before you begin

- The switch must be in Enhanced Secure mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable the USB port:

```
sys usb disable
```

3. Enable a previously disabled USB port:

```
no sys usb disable
```

Related links

[Chassis operations configuration using ACLI](#) on page 89

Chapter 10: Chassis operations configuration using EDM

This section provides the details to configure basic hardware and system settings using Enterprise Device Manager (EDM).

Editing system information

About this task

You can edit system information, such as the contact person, the name of the device, and the location to identify the equipment.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **System** tab.
5. Type the contact information in the **sysContact** field.
6. Type the system name in the **sysName** field.
7. Type the location information in the **sysLocation** field.
8. Click **Apply**.

System field descriptions

Use the data in the following table to use the **System** tab.

Name	Description
sysDescr	Shows the system assigned name and the software version.

Table continues...

Name	Description
sysUpTime	Shows the elapsed time since the system last started.
sysContact	Configures the contact information (in this case, an email address) for the Avaya support group.
sysName	Configures the name of this device.
sysLocation	Configures the physical location of this device.
DnsDomainName	Configures the default domain for querying the DNS server.
LastChange	Displays the time since the last configuration change.
LastVlanChange	Displays the time since the last VLAN change.
LastStatisticsReset	Displays the time since the statistics counters were last reset.
LastRunTimeConfigSave	Displays the last run-time configuration saved.
DefaultRuntimeConfigFileName	Displays the default Run-time configuration file directory name.
ConfigFileName	Specifies the name of a new configuration file.
ActionGroup1	Can be one of the following actions: <ul style="list-style-type: none"> • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration • loadLicense—loads a software license file to enable features
ActionGroup3	Can be the following action: <ul style="list-style-type: none"> • flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be the following action: <ul style="list-style-type: none"> • softReset—resets the device without running power-on tests
Result	Displays a message after you click Apply .

Editing chassis information

About this task

Edit the chassis information to make changes to chassis-wide settings.

Procedure

1. In the Device Physical View tab, select the Device.

2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Chassis** tab.
5. Edit the necessary options.
6. Click **Apply**.

Chassis field descriptions

Use the data in the following table to use the **Chassis** tab.

Name	Description
Type	Specifies the chassis type.
SerialNumber	Specifies a unique chassis serial number.
HardwareRevision	Specifies the current hardware revision of the device chassis.
NumSlots	Specifies the slot number as 1.
NumPorts	Specifies the number of ports currently installed in the chassis.
BaseMacAddr	Specifies the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
MacAddrCapacity	Specifies the MAC address capacity. The default value is 256.
Temperature	Specifies the temperature of the device.
MacFlapLimitTime	Configures the time limit for the loop-detect feature, in milliseconds, for MAC flapping. The value ranges from 10–5000. The default value is 500.
AutoRecoverDelay	Configures the delay in autorecovery. The value ranges from 5–3600. The default is 30 seconds.
MTUSize	Configures the maximum transmission unit size. The default is 1950.
MgidUsageVlanCurrent	Number of MGIDs for VLANs currently in use.
MgidUsageVlanRemaining	Number of remaining MGIDs for VLANs.
MgidUsageMulticastCurrent	Number of MGIDs for multicast currently in use.
MgidUsageMulticastRemaining	Number of remaining MGIDs for multicast.
DdmMonitor	Enables or disables the monitoring of the DDM. When enabled, the user gets the internal performance condition (temperature, voltage, bias, Tx power and Rx power) of the SFP/XFP. The default is disable.
DdmMonitorInterval	Configures the DDM monitor interval in the range of 5 to 60 in seconds. If any alarm occurs, the user gets the log message before the specific interval configured by the user. The default value is 5 seconds.

Table continues...

Name	Description
DdmTrapSend	Enables or disables the sending of trap messages. When enabled, the trap message is sent to the Device manager, any time the alarm occurs. The default is enable.
DdmAlarmPortdown	Sets the port down when an alarm occurs. When enabled, the port goes down when any alarm occurs. The default is disable.
PowerUsage	Specifies the amount of power the CPU uses.
PowerAvailable	Specifies the amount of power available to the CPU.

Configuring system flags

About this task

Configure the system flags to enable or disable flags for specific configuration settings.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. Select the system flags you want to activate.
6. Clear the system flags you want to deactivate.
7. Click **Apply**.

Important:

After you change certain configuration parameters, you must save the changes to the configuration file.

System Flags field descriptions

Use the data in the following table to use the **System Flags** tab.

Name	Description
EnableAccessPolicy	Activates access policies. The default is disabled.
ForceTrapSender	Configures circuitless IP as a trap originator. The default is disabled.

Table continues...

Name	Description
ForceIpHdrSender	If you enable Force IP Header Sender, the system matches the IP header source address with SNMP header sender networks. The default is disabled.
ForceTopologyIpFlagEnable	Activates or disables the flag that configures the CLIP ID as the topology IP. Values are true or false. The default is disabled.
CircuitlessIpId	Uses the CLIP ID as the topology IP. Enter a value from 1–256.

Configuring basic port parameters

About this task

Configure options for a basic port configuration.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, open the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. Click the **Interface** tab.
5. Configure the fields as required.

The 10/100BASE-TX ports do not consistently autonegotiate with older 10/100BASE-TX equipment. You can sometimes upgrade the older devices with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question. Check the Avaya web site for the latest compatibility information.

6. Click **Apply**.

Interface field descriptions

Use the data in the following table to use the **Interface** tab.

Name	Description
Index	Displays the index of the port, written in the slot/port format.
Name	Configures the name of the port.

Table continues...


Name	Description
Descr	Displays the description of the port. A textual string containing information about the interface.
Type	Displays the type of connector plugged in the port.
Mtu	Displays the Maximum Transmission Unit (MTU) for the port. The size of the largest datagram which can be sent or received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
PhysAddress	Displays the physical address of the port. The address of the interface at the protocol layer immediately 'below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
VendorDescr	Displays the vendor of the connector plugged in the port. This option is only applicable to ports 1/47 to 1/50.
AdminStatus	Configures the port as enabled (up) or disabled (down) or testing. The testing state indicates that no operational packets can be passed.
OperStatus	Displays the current status of the port. The status includes enabled (up) or disabled (down) or testing. The testing state indicates that no operational packets can be passed.
LastChange	Displays the timestamp of the last change.
LinkTrap	Enable or disable link trapping.
AutoNegotiate	<p>Enables or disables Autonegotiation for this port.</p> <p> Note:</p> <p>The 10 GigabitEthernet fiber-based I/O module ports can operate at either 1 Gigabit per second (Gbps) or 10 Gbps, dependent upon the capabilities optical transceiver that you install.</p> <p>This presents an ambiguity with respect to the autonegotiation settings of the port, while 1 Gigabit Ethernet (GbE) ports require autonegotiation; autonegotiation is not defined and is non-existent for 10 GbE ports.</p> <p>For a 10GbE fiber-based I/O module, you have the capability to swap back-and-forth between 1 GbE and 10 GbE operation by simply swapping transceivers. To help with this transition</p>

Table continues...

Name	Description
	<p>between 1 GbE and 10 GbE port operation, Avaya allows you to configure autonegotiation when you install a 10 GbE transceiver, even though autonegotiation is not defined for 10GbE.</p> <p>You can do this in anticipation of a port changeover from 10 GbE to 1 GbE. In this manner, you could essentially preconfigure a port in 1 GbE mode while the 10 GbE transceiver is still installed. The port is ready to go upon the changeover to the 1 GbE transceiver.</p> <p>In addition, you can use a saved configuration file with autonegotiation enabled to boot a system with either 10 GbE or 1 GbE transceivers installed. If you install a 1 GbE transceiver, the system applies autonegotiation. If you install a 10 GbE transceiver, the system does not remove the autonegotiation settings from the configuration, but the system simply ignores the configuration because autonegotiation settings are irrelevant to a 10 GbE transceiver. The system preserves the saved configuration for autonegotiation when resaved no matter which speed of transceiver you install.</p>
AdminDuplex	If AutoNegotiate is false, configures if the port should connect using full duplex or half duplex. The default is half.
OperDuplex	Displays the currently saved AdminDuplex value.
AdminSpeed	If AutoNegotiate is false, configures the speed of the port. The default is 10 Mb/s.
OperSpeed	Displays the currently saved AdminSpeed value.
AutoNegAd	<p>Configures the Custom Autonegotiation Advertisement (CANA) settings of the port.</p> <p>The abilities specified in this object are only used when auto-negotiation is enabled on the port. If all bits in this object are disabled, and auto-negotiation is enabled on the port, then the physical link process on the port will be disabled (if hardware supports this ability.)</p> <p>Any change in the value of this bit map will force the PHY to restart the auto-negotiation process. This will</p>

Table continues...

Name	Description
	<p>have the same effect as physically unplugging and reattaching the cable plant attached to the port.</p> <p>The capabilities being advertised are either all the capabilities supported by the hardware or the user-configured capabilities, which is a subset of all the capability supported by hardware.</p> <p>The default for this object will be all of the capabilities supported by the hardware.</p>
QoSLevel	Selects the Quality of Service (QoS) level for this port. The default is level1.
DiffServ	Enables the Differentiated Service feature for this port. The default is disabled.
Layer3Trust	Configures if the system should trust Layer 3 packets coming from access links or core links only. The default is core.
Layer2Override8021p	Specifies whether Layer 2 802.1p override is enabled (selected) or disabled (cleared) on the port. The default is disabled (clear).
MltId	Shows the MLT ID associated with this port. The default is 0.
Locked	Shows if the port is locked. The default is disabled.
UnknownMacDiscard	Discards packets that have an unknown source MAC address, and prevents other ports from sending packets with that same MAC address as the destination MAC address. The default is disabled.
DirectBroadcastEnable	Enables packets to broadcast directly.
HighSecureEnable	Enables or disables the high secure feature for this port.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
IpssecEnable	Enables or disables IP security (IPsec) on the interface. The default is disabled.
IngressRatePeak	Configures the peak rate in Kb/s. The default is 0.
IngressRateSvc	Configures the service rate in Kb/s. The default is 0.
EgressRateLimitState	Enables or disables egress port-based shaping to bind the maximum rate at which traffic leaves the port. The default is disabled.
EgressRateLimit	Configures the egress rate limit in Kb/s. VSP supports the range 10000 to 10000000. If configured to 0, it means this option is disabled.

Table continues...

Name	Description
Action	<p>Performs one of the following actions on the port</p> <ul style="list-style-type: none"> • none - none of the following actions • flushMacFdb - flush the MAC forwarding table • flushArp - flush the ARP table • flushIp - flush the IP route table • flushAll - flush all tables • clearLoopDetectAlarm - manually enable the port on all the disabled vlans. <p>The default is none.</p>
Result	Displays result of the selected action. The default is none.
IsPortShared	<p>Indicates whether the port is combo or not.</p> <ul style="list-style-type: none"> • portShared—Combo port. • portNotShared—Not a combo port.
PortActiveComponent	<p>Specifies whether the copper port is active or fabric port is active if port is a combo port.</p> <ul style="list-style-type: none"> • fixed port—Copper port is active. • gbic port—Fabric port is active.

Changing the boot configuration

Change the boot configuration to determine the services available after the system starts.

About this task

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) and Telnet server support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

On IPv6 networks, the switch supports SSHv2 server, remote login (rlogin) server and Remote Shell (rsh) server only. The switch does not support outbound SSHv2 client over IPv6, rlogin client over IPv6 or rsh client over IPv6. On IPv4 networks, the switch supports both server and client for SSHv2, rlogin and rsh.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Boot Config** tab.


5. Select the services you want to enable.
6. Click **Apply**.

Boot Config field descriptions

Use the data in the following table to use the **Boot Config** tab.

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time configuration.
PrimaryConfigSource	Specifies the primary configuration source.
PrimaryBackupConfigSource	Specifies the backup configuration source to use if the primary does not exist.
EnableFactoryDefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
EnableDebugMode	<p>Enables the debugmode to allow you to enable trace on any module by prompting the selection on the console during boot up. This allows the user to start trace for debugging earlier on a specified module. It only works on console connection. By default, it is disabled.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
EnableRebootOnError	<p>Activates or disables automatic reboot on a fatal error. The default value is activated.</p> <p>! Important: Do not change this parameter unless directed by Avaya.</p>
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled.
EnableRloginServer	Activates or disables the rlogin and rsh server. The default value is disabled.
EnableFtpServer	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the TFTP flag is disabled.
EnableTftpServer	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
EnableSshServer	Activates or disables the SSH server service. The default value is disabled.

Table continues...

Name	Description
EnableSpbmConfigMode	<p>Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.</p> <p>Use the no operator so that you can configure PIM and IGMP.</p> <p>The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.</p>
EnableEnhancedsecureMode	<p>Enables or disables the enhanced secure mode. The default is disabled.</p> <p>Select either jitc or non-jitc to enable the enhanced secure mode in one of these sub-modes.</p> <p> Note:</p> <p>The JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities. It is recommended that you use the non-JITC sub-mode.</p>

Viewing the boot configuration

About this task

View the boot configuration to determine the software version, as well as view the source from which the switch last started.

Procedure




1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Boot Config** tab.

Boot Config field descriptions

Use the data in the following table to use the **Boot Config** tab.

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time configuration.
PrimaryConfigSource	Specifies the primary configuration source.

Table continues...

Name	Description
PrimaryBackupConfigSource	Specifies the backup configuration source to use if the primary does not exist.
EnableFactoryDefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
EnableDebugMode	<p>Enables the debugmode to allow you to enable trace on any module by prompting the selection on the console during boot up. This allows the user to start trace for debugging earlier on a specified module. It only works on console connection. By default, it is disabled.</p> <p> Important: Do not change this parameter unless directed by Avaya.</p>
EnableRebootOnError	<p>Activates or disables automatic reboot on a fatal error. The default value is activated.</p> <p> Important: Do not change this parameter unless directed by Avaya.</p>
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled.
EnableRloginServer	Activates or disables the rlogin and rsh server. The default value is disabled.
EnableFtpServer	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the TFTPD flag is disabled.
EnableTftpServer	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
EnableSshServer	Activates or disables the SSH server service. The default value is disabled.
EnableSpbmConfigMode	<p>Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.</p> <p>Use the no operator so that you can configure PIM and IGMP.</p> <p>The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.</p>
EnableEnhancedsecureMode	<p>Enables or disables the enhanced secure mode. The default is disabled.</p> <p>Select either jitc or non-jitc to enable the enhanced secure mode in one of these sub-modes.</p> <p> Note: The JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities. It is recommended that you use the non-JITC sub-mode.</p>

Enabling Jumbo frames

About this task

Enable Jumbo frames to increase the size of Ethernet frames supported on the chassis.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Chassis** tab.
5. In **MTU size**, select either 1950, 9600 or 1522.
6. Click **Apply**.

Associating a port to a VRF instance

About this task

Associate a port to a Virtual Router Forwarding (VRF) instance so that the port becomes a member of the VRF instance.

You can assign a VRF instance to a port after you configure the VRF. The system assigns ports to the GlobalRouter, VRF 0, by default.

Procedure

1. In the **Device Physical** View tab, select a port.
2. In the navigation tree, open the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. Click the **VRF** tab.
5. To the right of the **BrouterVrflid** box, click the ellipsis (...) button.
6. In the BrouterVrflid dialog box, select the required VRF.
7. Click **OK**.
8. Click **Apply**.

Configuring the date and time

About this task

Configure the date and time to correctly identify when events occur on the system.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **User Set Time** tab.
5. Type and select the correct details.
6. Click **Apply**.

 **Note:**

According to a bill passed by the government of Russia, from October 2014 Moscow has moved from current UTC+4 into UTC+3 time zone with no daylight savings.

User Set Time field descriptions

Use the data in the following table to use the **User Set Time** tab.

Name	Description
Year	Configures the year (integer 1998–2097). The default is 1998.
Month	Configures the month. The default is 1.
Date	Configures the day (integer 1–31). The default is 1.
Hour	Configures the hour (12am–11pm). The default is 0.
Minute	Configures the minute (integer 0–59). The default is 0.
Second	Configures the second (integer 0–59). The default is 0.
Time Zone	Configures the time zone.

Auto reactivating the port of the SLPP shutdown

About this task

Use the following procedure to auto reactivate the port which is shut down by the SLPP.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, open the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. Click the **CP Limit** tab.
5. Select **AutoRecoverPort** to activate auto recovery of the port from the action taken by SLPP shutdown features. The default value is disabled.
6. Click **Apply**.

Editing serial port parameters

About this task

Perform this procedure to specify serial port communication settings. The serial port on the device is the console port.

Procedure

1. In the Device Physical View tab, select the console port on the device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Serial Port**.
4. Edit the port parameters as required.

Serial Port field descriptions

Use the data in the following table to use the **Serial Port** tab.

Name	Description
IfIndex	Specifies the slot and port number for the serial port.
BaudRate	Specifies the baud rate of this port. The default is 9600.
DataBits	Specifies the number of data bits, for each byte of data, this port sends and receives. The default is 7.

Enabling port lock

About this task

Use the port lock feature to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify locked ports until you first unlock the port.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. To enable port lock, select the **Enable** check box.
5. Click **Apply**.

Port Lock field descriptions

Use the data in the following table to use the **Port Lock** tab.

Name	Description
Enable	Activates the port lock feature. Clear this check box to unlock ports. The default is disabled.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Locking a port

Before you begin

- You must enable port lock before you lock or unlock a port.

About this task

Use the port lock feature to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify locked ports until you first unlock the port.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. In the **LockedPorts** box, click the ellipsis (...) button.

5. Click the desired port or ports.
6. Click **Ok**.
7. In the Port Lock tab, click **Apply**.

Port Lock field descriptions

Use the data in the following table to use the **Port Lock** tab.

Name	Description
Enable	Activates the port lock feature. Clear this check box to unlock ports. The default is disabled.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Viewing power information

About this task

View power information to see the amount of power available and used by the chassis and all components.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Power Info** tab.

Power Info field descriptions

Use the data in the following table to use the **Power Info** tab.

Name	Description
TotalPower	Shows the total power for the chassis.
RedundantPower	Shows the redundant power for the chassis.
PowerUsage	Shows the power currently used by the complete chassis.
PowerAvailable	Shows the unused power.

Viewing fan information

About this task

View fan information to monitor the alarm status of the cooling modules in the chassis.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **Fan Info** tab.

Fan Info field descriptions

Use the data in the following table to use the **Fan Info** tab.

Name	Description
Id	Specifies the fan ID.
Status	Specifies the operation status of the F\fan.
AmbientTemperature	Specifies the temperature of the fan.
Type	Specifies the running speed type of the fan.

Viewing USB information

About this task

View USB information.

Important:

This procedure is applicable only to the VSP 4850GTS Series.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **USB** tab.

Viewing topology status information

About this task

View topology status information (which includes Avaya Management MIB status information) to view the configuration status of the SynOptics Network Management Protocol (SONMP) on the system.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > Diagnostics**.
2. Click **Topology**.
3. Click the **Topology** tab.

Topology field descriptions

Use the data in the following table to use the **Topology** tab.

Name	Description
IpAddr	Specifies the IP address of the device.
Status	Indicates whether topology (SONMP) is on or off for the device.
NmmLstChg	Specifies the value of sysUpTime, the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified, if the table did not change since the last cold or warm start of the agent.
NmmMaxNum	Specifies the maximum number of entries in the NMM topology table.
NmmCurNum	Specifies the current number of entries in the NMM topology table.

Viewing the topology message status

About this task

View topology message status to view the interconnections between Layer 2 devices in a network.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > Diagnostics**.
2. Click **Topology**.
3. Click the **Topology Table** tab.

Topology Table field descriptions

Use the data in the following table to use the **Topology Table** tab.

Name	Description
Slot	Specifies the slot number in the chassis that received the topology message.
Port	Specifies the port that received the topology message.
IpAddr	Specifies the IP address of the sender of the topology message.
SegId (RemPort)	Specifies the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Specifies the MAC address of the sender of the topology message.
ChassisType	Specifies the chassis type of the device that sent the topology message.
BkplType	Specifies the backplane type of the device that sent the topology message. Avaya Virtual Services Platform uses a backplane type of 12.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Specifies the current state of the sender of the topology message. The choices are <ul style="list-style-type: none"> • topChanged—Topology information recently changed. • heartbeat—Topology information is unchanged. • new—The sending agent is in a new state.

Configuring a forced message control pattern

About this task

Configure a forced message control pattern to enforce configured message control actions.

Procedure

1. In the navigation pane, expand the following folders: **Configuration > Edit > Chassis**.
2. Click the **Force Msg Patterns** tab.
3. Click **Insert**.
4. In the **PatternId** field, enter a pattern ID number.
5. In the **Pattern** field, enter a message control pattern.
6. Click **Insert**.

Force Msg Patterns field descriptions

Use the data in the following table to use the **Force Msg Patterns** tab.

Name	Description
PatternId	Specifies a pattern identification number in the range 1–32.
Pattern	Specifies a forced message control pattern of 4 characters. The software and the hardware log messages that use the first four bytes matching one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****). If you specify the wildcard pattern, all messages undergo message control.

Chapter 11: Power over Ethernet fundamentals

Power over Ethernet (PoE) is the implementation of IEEE 802.3at which allows for both data and power to pass over a copper Ethernet LAN cable. Typical power devices include wireless Access Points and VoIP telephones.

PoE is supported on the switch on copper ports 1 to 48. This includes the combination copper ports 47 and 48. PoE is not supported on the fiber slots 47 and 48, or the SFP+ slots 49 and 50.

The switch uses the Dynamic Power Allocation scheme when supplying power to devices. Only the actual power being consumed by the device is allocated, improving efficiency and allowing for more devices to be supported.

You can configure PoE from CLI and Enterprise Device Manager (EDM). For details, see the following sections.

Related links

[PoE overview](#) on page 119

[PoE detection types](#) on page 120

[Power usage threshold](#) on page 121

[Port power limit](#) on page 121

[Port power priority](#) on page 121

PoE overview

You can plug any IEEE802.3af-compliant or IEEE802.3at-compliant for PWR+ powered device into a front-panel port and receive power in that port. Data also can pass simultaneously on that port. This capability is called PoE.

For more information about PoE and power supplies, see *Installing Avaya Virtual Services Platform 4850GTS Series*, NN46251-300.

The IEEE 802.3af draft standard regulates a maximum of 15.4 W of power for each port; that is, a power device cannot request more than 15.4 W of power. As different network devices require different levels of power, the overall available power budget of the switch depends on your power configuration and the particular connected network devices. If you connect an IP device that requires more than 16 W of power, you see an error on that port notifying you of an overload.

The VSP 4850GTS-PWR+ switch automatically detects each IEEE 802.3af-draft-compliant powered device attached to each front-panel port and immediately sends power to that appliance. The switch also automatically detects how much power each device requires and supply the required DC voltage at a set current based on the load conditions and current availability. The switch supports both PoE and standard LAN devices.

The VSP 4850GTS-PWR+ switch automatically detects any IEEE 802.3at-compliant powered device attached to any PoE front panel port and immediately sends power to that appliance.

The power detection function of the VSP 4850GTS-PWR+ switch operates independently of the data link status. A device that is already operating the link for data or a device that is not yet operational can request power. That is, the switch provides power to a requesting device even if the data link for that port is disabled. The switch monitors the connection and automatically disconnects power from a port when you remove or change the device, as well as when a short occurs.

The switch automatically detects devices that require no power connections from them, such as laptop computers or other switching devices, and sends no power to those devices. You control the supply of power to specific ports by setting the maximum allowed power to each port in 1 W increments, from 3 W to 32W.

! Important:

Allow 30 seconds between unplugging and replugging an IP device to the switch to enable the IP device to discharge. If you attempt to connect earlier, the switch may not detect the IP device.

The VSP 4850GTS-PWR+ switch provides the capability to set a PoE power threshold, which lets you set a percentage of the total PoE power usage at which the switch sends a warning message. If the power consumption is below the threshold, the switch logs an information message.

Related links

[Power over Ethernet fundamentals](#) on page 119

PoE detection types

The global configured detection type specifies the following versions of the IEEE to support:

Detection Type	Power Mode
802.3af	Normal
802.3af and legacy	Normal
802.3at	High
802.3at and legacy	High

By default, 802.3at (including legacy) is the POE PD detection type. In this high power mode, Class 4 PDs receive up to 32 watts of power.

*** Note:**

802.3at is backwards compatible with 802.3af. Hence, both normal power and high power devices are supported in this mode.

802.3af is the older standard and allows up to 16 watts of power.

*** Note:**

Changing from 802.3at to 802.3af is permitted, however power delivery is interrupted during this operation, and all PoE devices are reset. There is no service interruption when changing from 802.3af to 802.3at.

Related links

[Power over Ethernet fundamentals](#) on page 119

Power usage threshold

The power usage threshold is a chassis configurable percent of the total power available on the switch. When the POE power consumption exceeds this threshold, a log message is generated to warn such an event. When power consumption transitions below the threshold, an informational log message is logged. The default threshold is 80%.

Related links

[Power over Ethernet fundamentals](#) on page 119

Port power limit

Each POE port has a configurable power limit. This configuration attribute is a mechanism to limit the amount of power supplied on a particular port. By default, all ports have a limit of 32 watts which is the maximum. If a PD requires more than the configured limit, the device may not connect properly or is forced to run at a lower limit.

Related links

[Power over Ethernet fundamentals](#) on page 119

Port power priority

You can configure the power priority of each port by choosing low, high, or critical power priority settings.

The switch automatically drops low-priority ports when the power requirements exceed the available power budget. When the power requirements becomes lower than the switch power budget, the power returns to the dropped port. When several ports have the same priority and the power budget is exceeded, the ports with the highest interface number are dropped until the consumption is within the power budget.

The priority methods are:

1. Port configured PoE priority

- Low: (default) standard priority for standard devices
- High: higher priority than low for important devices
- Critical: highest priority for critical devices like wireless APs

2. Port number priority where the lower port numbers have a higher priority.

PD Classification

The PDs are classified into a Class 0 – 4 during initial connection establishment as defined in IEEE 802.3at / 802.3af. The classification defines the amount of power the device is expected to consume.

Table 33: Classification chart for 802.3at

Class	Min PSE Power	Example PD
0	15.4 watts	
1	4 watts	IP Phones
2	7 watts	IP Camera
3	15.4 watts	Wireless AP
4	30 watts	High Power PD

Table 34: Classification chart for 802.3af

Class	Min PSE Power	Example PD
1	4 watts	IP Phones
2	7 watts	IP Camera
3, 4 or 0	15.4 watts	Wireless AP

Related links

[Power over Ethernet fundamentals](#) on page 119

Chapter 11: PoE/PoE+ Allocation Using LLDP

Power over Ethernet/Power over Ethernet Plus allocation using Link Layer Discovery Protocol (LLDP) is supported on the VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR+ Ethernet Switches. These two switches support IEEE-based PoE and play the role of power sourcing equipment (PSE).

The devices that are powered using PoE/PoE+, such as IP Phone and Video Surveillance Cameras, are classified as Powered Devices (PD). The maximum allowed continuous output power per cable in the original 802.3af PoE specification is 15.4 watts, while the enhanced 802.3at PoE+ specification allows for up to 25.5 watts. The negotiation of actual power supply and demand between a PSE and a PD can be executed at either the physical layer or at the data link layer. After link is established at the physical layer, the PSE can use the IEEE 802.1AB LLDP protocol to repeatedly query the PD to discover its power needs. Communication using LLDP allows for a finer control of power allocation, making it possible for the PSE to dynamically supply the exact power levels needed by individual PDs, and globally for all PDs that are attached. Using LLDP is optional for the PSE, however, it is mandatory for a Type 2 PD that requires more than 12.95 watts of power.

Important:

LLDP is introduced to support PoE discovery and power allocation in the current release because the VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR+ products do not support hardware-level power negotiation. This introduction allows Type 2 PDs such PTZ (pan-tilt-zoom) Video Surveillance Cameras to be fully functional when connected to one of these Switches. This functionality is enabled by default and is not configurable.

Note:

The VSP 4450GSX-PWR+ Ethernet Switch features a hardware design that supports hardware-level detection. Therefore, does not require LLDP.

Chapter 12: Power over Ethernet configuration using ACLI

Power over Ethernet (POE) is supported on the VSP4850GTS-PWR+ chassis. This section provides details to configure PoE settings using ACLI.

Related links

- [Disable PoE on a port](#) on page 124
- [Configuring PoE detection type](#) on page 125
- [Configuring PoE power usage threshold](#) on page 126
- [Configuring power limits for channels](#) on page 126
- [Configuring port power priority](#) on page 127
- [Displaying PoE main configuration](#) on page 128
- [Displaying PoE port status](#) on page 128
- [Displaying port power measurement](#) on page 129

Disable PoE on a port

About this task

Disable PoE on a port.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interfaceGigabitEthernet {slot/port[-slot/port][, ...]} OR interface
vlan <1-4084>
```

2. Disable PoE on the port:

```
poe poe-shutdown [port <portlist>]
```

<portlist> is the port on which you want to disable PoE. The default is enable.

Next steps

To return power to the port, enter `no poe-shutdown [port <portlist>]`.

Related links

[Power over Ethernet configuration using ACLI](#) on page 124

Configuring PoE detection type

The `poe-pd-detect-type` command enables either 802.3af and Legacy compliant PD detection methods, or 802.3at and Legacy compliant PD detection methods. The default detection type is 802.3at and legacy.

- 802.3af : normal power mode
- 802.3af and legacy
- 802.3at : high power mode
- 802.3at and legacy

802.3at is backwards compatible with 802.3af. Therefore, both normal power and high power devices are supported in 802.3at.

Note:

Changing from 802.3at to 802.3af is permitted, however power delivery is interrupted during this operation, and all PoE devices are reset. There is no service interruption when changing from 802.3af to 802.3at.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure PoE detection type:

```
poe poe-pd-detect-type {802dot3af | 802dot3af_and_legacy | 802dot3at
| 802dot3at_and_legacy}
```

Variable definitions

Use the data in the following table to use the `poe-pd-detect-type` command.

Table 35: Variable definitions

Variable	Value
{802dot3af 802dot3af_and_legacy 802dot3at 802dot3at_and_legacy}	<ul style="list-style-type: none"> • 802dot3af: Set PD detection mode in 802.3af • 802dot3af_and_legacy: Set PD detection mode in 802.3af and legacy • 802dot3at: Set PD detection mode in 802.3at • 802dot3at_and_legacy: Set PD detection mode in 802.3at and legacy

Configuring PoE power usage threshold

About this task

The **poe-power-usage-threshold** command configures the power usage threshold in percentage on the switch. When the percentage is exceeded, the switch logs a warning message. When power consumption is below the threshold, the switch logs an informational message.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the power usage threshold:

```
po e poe-power-usage-threshold <1-99>.
```

Variable definitions

Use the data in the following table to use the **po e poe-power-usage-threshold** command.

Table 36: Variable definitions

Variable	Value
<1-99>	1—99 percent

Configuring power limits for channels

About this task

The `poe-limit` command sets the power limit for channels.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interfaceGigabitEthernet {slot/port[-slot/port][,...]} OR interface
vlan <1-4084>
```

2. Configure PoE channel limits:

```
poe poe-limit [port <portlist>] <3-32>
```

Variable definitions

Use the data in the following table to use the `poe-limit` command.

Table 37: Variable definitions

Variable	Value
<code><portlist></code>	Identifies the ports to set the limit on.
<code><3-32></code>	The power range for VSP4850GTS PWR+ units is 3 to 32W.

Configuring port power priority

About this task

The `poe-priority` command sets the port power priority.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interfaceGigabitEthernet {slot/port[-slot/port][,...]} OR interface
vlan <1-4084>
```

2. Configure port power priority:

```
poe poe-priority [port <portlist>] {critical| high| low}
```

Variable definitions

Use the data in the following table to use the `poe-priority` command.

Table 38: Variable definitions

Variable	Value
<portlist>	Identifies the ports to set priority for.
{low high critical}	Identifies the PoE priority.

Displaying PoE main configuration

About this task

Use this procedure to display the main PoE configuration.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. Enter `show poe-main-status`.

Example

```
#show poe-main-status
```

```
=====
                                PoE Main Status - Stand-alone
=====
Available DTE Power           : 1855 Watts
DTE Power Status              : NORMAL
DTE Power Consumption         : 92 Watts
DTE Power Usage Threshold     : 80
PD Detect Type                : 802.3at and Legacy
Power Source Present          : AC Only
Primary Power Status          : Present and operational
Redundant Power Status        : Present and Operational
```

Related links

[Power over Ethernet configuration using ACLI](#) on page 124

Displaying PoE port status

About this task

Use this procedure to display the PoE port status.

Procedure

1. Enter the Privileged EXEC mode:
enable
2. Enter **show poe-port-status**.

Example

```
#show poe-port-status
=====
                        POE Port Status
=====
PORT      ADMIN   CURRENT          LIMIT          PRIORITY
STATUS   STATUS   STATUS           CLASSIFICATION (Watts)
-----
1/1       Enable  DeliveringPower  Class0         32         Low
1/2       Enable  DeliveringPower  Class0         32         Low
1/3       Enable  DeliveringPower  Class4         32         High
1/4       Enable  Searching        Class0         32         Low
1/5       Enable  Searching        Class0         32         Low
1/6       Enable  DeliveringPower  Class4         32         Low
1/7       Enable  DeliveringPower  Class3         32         Critical
1/8       Enable  DeliveringPower  Class2         32         Low
1/9       Enable  Searching        Class0         32         Low
1/10      Enable  Searching        Class0         32         Low
1/11      Enable  Searching        Class0         32         Low
1/12      Enable  Searching        Class0         32         Low
1/13      Enable  Searching        Class0         32         Low
1/14      Enable  Searching        Class0         32         Low
1/15      Enable  Searching        Class0         32         Low
1/16      Enable  Searching        Class0         32         Low
1/17      Enable  Searching        Class0         32         Low
```

*** Note:**

The PoE status of all the 48 ports is displayed.

Related links

[Power over Ethernet configuration using ACLI](#) on page 124

Displaying port power measurement

About this task

Use this procedure to display the PoE power measurement.

Procedure

1. Enter the Privileged EXEC mode:
enable
2. Enter **show poe-power-measurement**.

Example

```
#show poe-power-measurement
=====
                                POE Port Measurement
=====
PORT  Volt (V)  CURRENT (mA)  POWER(Watt)
-----
1/1   34.0       117           6.200
1/2   34.0       94            5.000
1/3   34.0       535           28.500
1/4   0.0        0             0.000
1/5   0.0        0             0.000
1/6   34.0       525           27.900
1/7   34.0       152           8.100
1/8   34.0       49            2.600
```

*** Note:**

The PoE port measurement for all the 48 ports is displayed.

Related links

[Power over Ethernet configuration using ACLI](#) on page 124

Chapter 13: Power over Ethernet configuration using EDM

This section provides details to configure PoE settings using EDM.

Related links

[Configuring PoE globally](#) on page 131

[Viewing PoE information for specific switch ports using EDM](#) on page 133

Configuring PoE globally

About this task

Modify global PoE configuration.

Procedure

1. In the Device Physical View, select one or more ports.

 **Note:**

PoE is not supported on ports 49 and 50.

2. In the navigation tree, open the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. In the work area, click the **PoE** tab.
5. Select the **AdminEnable** checkbox.
6. Select a value from the list—true to enable PoE for the port, or false to disable PoE for the port.
7. Select one of the following values to for **PowerPriority**:
 - critical
 - high
 - low
8. Enter the value of the power in the **PowerLimit(watts)** field.
9. To configure PoE for other selected ports, repeat steps 6 through 8.

10. Click **Apply**.

Related links

[Power over Ethernet configuration using EDM](#) on page 131

[PoE field descriptions](#) on page 132

PoE field descriptions

Use the data in the following table to configure the PoE settings for specific ports.

Name	Description
Port	Shows the switch port number.
AdminEnable	Shows whether PoE is enabled or disabled on this port.
DetectionStatus	Shows the operational status of the powerdevice detecting mode on the specified port: <ul style="list-style-type: none"> • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault
PoweClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Shows the power priority for the specified: <ul style="list-style-type: none"> • critical • high • low
PoweerLimit(Watts)	Shows the maximum power that the switch can supply to a port. The maximum power and system default power is 32W per port.
Voltage(volts)	Shows the power measured in volts.
Current(amps)	Shows the power measured in amps.
Power(Watts)	Shows the power measured in watts.

Related links

[Configuring PoE globally](#) on page 131

Viewing PoE information for specific switch ports using EDM

About this task

View the PoE configuration for specific switch ports

Procedure

1. In the Device Physical View, select one or more ports.

*** Note:**

PoE is not supported on ports 49 and 50.

2. In the navigation tree, open the following folders: **Configuration > Edit > Port**.
3. Click **General**.
4. In the work area, click the **PoE** tab.

Related links

[Power over Ethernet configuration using EDM](#) on page 131

[PoE field descriptions](#) on page 133

PoE field descriptions

Use the data in the following table to display the PoE configuration for specific ports.

Name	Description
Port	Shows the switch port number.
AdminEnable	Shows whether PoE is enabled or disabled on this port.
DetectionStatus	Shows the operational status of the powerdevice detecting mode on the specified port: <ul style="list-style-type: none"> • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault
PoweClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption.

Table continues...

Name	Description
	Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Shows the power priority for the specified: <ul style="list-style-type: none">• critical• high• low
PowerLimit(Watts)	Shows the maximum power that the switch can supply to a port. The maximum power and system default power is 32W per port.
Voltage(volts)	Shows the power measured in volts.
Current(amps)	Shows the power measured in amps.
Power(Watts)	Shows the power measured in watts.

Related links

[Viewing PoE information for specific switch ports using EDM](#) on page 133

Chapter 14: Hardware status using EDM

This section provides methods to check the status of basic hardware in the chassis using Enterprise Device Manager (EDM).

Configuring polling intervals

About this task

Enable and configure polling intervals to determine how frequently EDM polls for port and LED status changes or detects the hot swap of installed modules.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Device**.
2. Click **Preference Setting**.
3. Enable polling.
4. Configure the frequency to poll the device.
5. Click **Apply**.

Preference Setting field descriptions

Use the data in the following table to use the **Preference Setting** tab.

Name	Description
Enable	Enables polling for port and LED status changes. The default is disabled.
Poll Interval	Specifies the polling interval, if enabled. The default is 60 seconds.

Viewing power supply parameters

About this task

Perform this procedure to view information about the operating status of the power supplies.

Procedure

1. In the Device Physical View tab, select a power supply.
2. In the navigation tree, open the following folders: **Configuration > Edit**.
3. Click **Power Supply**.
4. Click the **Detail** tab.

Detail field descriptions

Use the data in the following table to use the **Detail** tab.

Name	Description
Type	Describes the type of power used—AC or DC.
Description	Provides a description of the power supply.
SerialNumber	Specifies the power supply serial number.
HardwareRevision	Specifies the hardware revision number.
PartNumber	Specifies the power supply part number.
PowerSupplyOperStatus	Specifies the status of the power supply as one of the following: <ul style="list-style-type: none"> • on (up) • off (down)
InputLineVoltage	Specifies the input line voltage. Two possible states exist: <ul style="list-style-type: none"> • low 110v—power supply connected to a 110 Volt source • high 220v—power supply connected to a 220 Volt source <p>If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage shows the low 110v value.</p>
OutputWatts	Displays the output power of this power supply.

Viewing temperature on the chassis

You can view information about the temperature on the chassis.

About this task

The system triggers an alarm when one of the zones exceeds the threshold temperature value, and clears the alarm after the zone temperature falls below the threshold value.

When an elevated temperature triggers a temperature alarm, the fan speed increases, and the LED color changes on the front panel of the switch.

Procedure

1. In the Device Physical View tab, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Temperature** tab.

Temperature field descriptions

Use the data in the following table to use the **Temperature** tab.

Name	Description
CpuTemperature	Current CPU temperature in Celsius.

Chapter 15: DNS fundamentals

This section provides conceptual material on the Domain Name Service (DNS) implementation for Avaya Virtual Services Platform 4000 Series. Review this content before you make changes to the configurable DNS options.

DNS client

Every equipment interface connected to a Transmission Control Protocol over IP (TCP/IP) network is identified with a unique IPv4 or IPv6 address. You can assign a name to every machine that uses an IPv4 or IPv6 address. The TCP/IP does not require the usage of names, but these names make the task easier for network managers in the following ways:

- An IP client can contact a machine with its name, which is converted to an IP address, based on a mapping table. All applications that use this specific machine do not depend on the addressing scheme.
- It is easier to remember a name than a full IP address.

To establish the mapping between an IP name and an IPv4 or an IPv6 address you use the Domain Name Service (DNS). DNS is a hierarchical database that you can distribute on several servers for backup and load sharing. After you add a new hostname, update this database. The information is sent to all the different hosts. An IP client that resolves the mapping between the hostname and the IP address sends a request to one of the database servers to resolve the name.

After you establish the mapping of IP name and IP address, the application is modified to use a hostname instead of an IP address. The switch converts the hostname to an IP address.

If the entry to translate the hostname to IP address is not in the host file, the switch queries the configured DNS server for the mapping from hostname to IP address. You can configure connections for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary.

DNS modifies Ping, Telnet, and copy applications. You can enter a hostname or an IP address to invoke Ping, Telnet, and copy applications.

A log/debug report is generated for all the DNS requests sent to DNS servers and all successful DNS responses received from the DNS servers.

IPv6 support

The Domain Name Service (DNS) used by the Avaya Virtual Services Platform 4000 supports both IPv4 and IPv6 addresses with no difference in functionality or configuration.

Chapter 16: DNS configuration using ACLI

This section describes how to configure the Domain Name Service (DNS) client using Avaya command line interface (ACLI).

DNS supports IPv4 addresses.

Configuring the DNS client

About this task

Configure the Domain Name Service to establish the mapping between an IP name and an IPv4 address.

You can configure connection for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the DNS client:

```
ip domain-name WORD<0-255>
```

3. Optionally, add addresses for additional DNS servers:

```
ip name-server <primary|secondary|tertiary> WORD<0-46>
```

4. View the DNS client system status:

```
show ip dns
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
```

Add addresses for additional DNS servers:

```
VSP-4850GTS-PWR+:1(config)#ip name-server tertiary
fe80::221:5aff:fe68:c98d
```

Variable definitions

Use the data in the following table to use the `ip domain-name` command.

Table 39: Variable definitions

Variable	Value
<code>WORD<0–255></code>	Configures the default domain name. <code>WORD<0–255></code> is a string 0–255 characters.

Use the data in the following table to use the `ip name-server` command.

Table 40: Variable definitions

Variable	Value
<code>primary secondary tertiary WORD<0–46></code>	Configures the primary, secondary, or tertiary DNS server address. Enter the IP address in a.b.c.d format for IPv4 or hexadecimal format (string length 0–46) you cannot specify all three servers in one command. Use the <code>no</code> operator before this parameter, <code>no ip name-server <primary secondary tertiary></code>

Querying the DNS host

About this task

Query the DNS host for information about host addresses.

You can enter either a hostname, an IPv4 address. If you enter the hostname, this command shows the IP address that corresponds to the hostname and if you enter an IP address, this command shows the hostname for the IP address. DNS supports IPv4 addresses with no difference in functionality or configuration using ACLI.

Procedure

1. Enter the Privileged EXEC mode:

```
enable
```

2. View the host information:

```
show hosts WORD<0–256>
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

View the host information:

```
VSP-4850GTS-PWR+:1(config)#show hosts 10.10.10.1
```

Variable definitions

Use the data in the following table to use the `show hosts` command.

Table 41: Variable definitions

Variable	Value
<code>WORD<0-256></code>	Specifies one of the following: <ul style="list-style-type: none">• the name of the host DNS server as a string of 0–256 characters.• the IP address of the host DNS server in a.b.c.d format.

Chapter 17: DNS configuration using EDM

This section describes how to configure the Domain Name Service (DNS) using Enterprise Device Manager (EDM).

DNS supports IPv4. Under the **DNS Servers** tab, in the **DnsServerListAddressType** box, you must select **ipv4**.

Configuring the DNS client

About this task

You can configure connections for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary.

DNS supports IPv4 addresses. Under the **DNS Servers** tab, in the **DnsServerListAddressType** box, you must select **ipv4**.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > Diagnostics**.
2. Click **DNS**.
3. Click the **DNS Servers** tab.
4. Click **Insert**.
5. In the **DnsServerListType** box, select the DNS server type.
6. In the **DnsServerListAddressType** box, select the IP version.
7. In the **DnsServerListAddress** box, enter the DNS server IP address.
8. Click **Insert**.

DNS Servers field descriptions

Use the data in the following table to use the **DNS Servers** tab.

Name	Description
DnsServerListType	Configures the DNS server as primary, secondary, or tertiary.
DnsServerListAddressType	Configures the DNS server address type as IPv4.
DnsServerListAddress	Specifies the DNS server address.
DnsServerListStatus	Specifies the status of the DNS server.
DnsServerListRequestCount	Specifies the number of requests sent to the DNS server.
DnsServerListSuccessCount	Specifies the number of successful requests sent to the DNS server.

Querying the DNS host

About this task

Query the DNS host for information about host addresses.

You can enter either a hostname or an IPv4 address. If you enter the hostname, this command shows the IP address that corresponds to the hostname and if you enter an IP address, this command shows the hostname for the IP address. DNS supports IPv4 addresses with no difference in functionality or configuration in this procedure.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit > Diagnostics**.
2. Click **DNS**.
3. Click the **DNS Host** tab.
4. In the **HostData** text box, enter the DNS host name, IPv4 address.
5. Click **Query**.

DNS Host field descriptions

Use the data in the following table to use the **DNS Host** tab.

Name	Description
HostData	Identifies the host name or the host IPv4 address . This variable is a read-only field.
HostName	Identifies the host name. This variable is a read-only field.
HostAddressType	Identifies the address type of the host.
HostAddress	Identifies the host IP address. This variable is a read-only field.
HostSource	Identifies the DNS server IP or host file. This variable is a read-only field.

Chapter 18: Licensing fundamentals

This section provides conceptual information about feature licensing for Avaya Virtual Services Platform 4000 Series. Review this section before you make changes to the license configuration.

Feature licensing

! Important:

Prior to VOSS 4.1, VSP 4000 used the Avaya Data Licensing Portal to generate license files. This system produced a license file with the `.dat` extension. In VOSS 4.1 and later, VSP 4000 uses the Product Licensing and Delivery System (PLDS) as the license order, delivery, and management tool. PLDS produces a license file with the `.xml` extension. If you have older `.dat` license files on your switch, the software continues to support them. For more information, see [Transition to PLDS](#) on page 147.

PLDS provides self-service license activations, upgrades, moves and changes.

* Note:

PLDS supports only a single host (system MAC address) for each license file. You cannot use the same license file on multiple hosts.

Premier License

The switch requires a Premier License for Layer 3 VSNs (including Multicast), Fabric Extend and MACsec features. These are in addition to the features covered by the Base License.

Because MACsec is not allowed in some countries, Avaya offers the following PLDS licenses with and without MACsec:

- **PLDS Premier License** – This license is required to enable and use the following features:
 - Avaya Fabric Connect Layer 3 Virtual Services Networks (VSNs)
 - Avaya Fabric Extend including the use of logical IS-IS interfaces
- **PLDS Premier License plus MACsec** – This license is required to enable and use the following features:
 - Avaya Fabric Connect Layer 3 Virtual Services Networks (VSNs)
 - Avaya Fabric Extend including the use of logical IS-IS interfaces
 - IEEE 802.1AE MACsec

- **PLDS Premier License to PLDS Premier License plus MACsec Uplift** – This license is for customers that want to upgrade their Premier License to a Premier License plus MACsec.

Premier Trial License:

For customers that would like to trial premier features prior to purchasing a Premier License, there are the following two types of PLDS Premier trial licenses that permit the use of premier features for a 60 day period. During the trial period you can configure all features without restriction, including system console and log messages.

- **PLDS Premier Trial License** – This license is for Layer 3 VSNS including Multicast and Fabric Extend, but you cannot configure MACsec.
- **PLDS Premier Trial License plus MACsec** – This license is for MACsec and Layer 3 VSNS including Multicast and Fabric Extend.

The PLDS Premier Trial License is generated using the system MAC address of a switch and can only be generated and used *once* for a given MAC address.

System console and log messages alert you to the expiry of the 60 day trial period. The message `Licence trial period will expire in ## days` appears every 24 hours. At the end of the trial period, the following message appears: `License trial period has expired. All the Premier features will be disabled. Please buy the license to enable them.` This message is the last notification recorded.

The system logs the preceding messages even if you do not use or test license features during the trial period. If you load a valid license on the system, it does not record the preceding messages.

After the expiry of the 60 day trial period, you will also see messages in the alarms database that the license has expired. If you restart the system after the license expiration, the Premier features will not be loaded even if they are in the saved configuration.

If you purchase a Premier License, you must obtain and install a license file. For more information about how to generate and install a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300. All licensing activities are performed through the Avaya PLDS Portal at <http://plds.avaya.com>. For more information about the transition to the PLDS system, see [Transition to PLDS licensing](#) on page 147.

Base License

The Base License is included with the VSP 4000 hardware and the ERS 4850 to VSP 4000 Conversion kit, and activates the features not included in the Premier License.

The Base License includes the following Layer 2 features:

- VLANs
- RSTP
- MSTP
- MLT
- IGMP
- 802.1AX Link Aggregation (LACP)
- 802.1ag
- SPB Core/Base (NNI)
- Layer 2 Virtual Service Networks (VSNS)

- Etree
- Layer 2 Virtual Service Networks (VSN) with Multicast
- Virtualized Multicast over Fabric Connect*
- Fabric Attach
- Switched UNI (S-UNI)

The Base License includes the following Layer 3/ Routing features:

- Global Routing Table (GRT) IP Routing including IP-Shortcuts
- Terminal Access Controller Access Control System Plus (TACACS+)
- Service Level Agreement Monitor (SLA Mon™)
- Inter-ISID-Routing
- VRRP
- DHCP-Relay
- RIP in the GRT and VRF
- RIP in the GRT with IP Shortcuts
- OSPF in the GRT and VRF
- OSPF in the GRT with IP Shortcuts
- BGP in the GRT and VRF
- BGP in the GRT with IP Shortcuts
- SPB in the GRT with IP Shortcuts
- Multicast using IP-Shortcuts
- GRT with IP Shortcuts
- Route Policy Virtualization in the GRT and the GRT with IP Shortcuts
- IP Multicast Routing parity with IGMP v1, v2, and v3
- IP VRF
- IPv6
- IPv6 Alternative Routes
- SMLT
- Switched UNI (S-UNI)
- Per-queue Rate Limiting

License type and part numbers

The following table provides the part number for the various licenses supported on Virtual Services Platform 4000.

Table 42: Supported licenses

Part number/Order code	License type
338835	Virtual Services Platform 4000 PLDS Premier License w/MACsec - 1 Unit
338836	Virtual Services Platform 4000 PLDS Premier License - 1 Unit
339241	Virtual Services Platform 4000 PLDS Premier Trial License
339541	Virtual Services Platform 4000 PLDS Premier Trial License w/MACsec
339542	Virtual Services Platform 4000 PLDS Premier to Premier w/MACSEC UPLIFT LIC

Feature license files

After you obtain the license file to enable Premier License features, you must install the license file on the system to unlock the associated licensed features. For Virtual Services Platform 4000, you must load a license file on the internal flash of the device (`/intflash/`).

Transition to PLDS

The section provides information about the transition from the original three-tier licensing system to the new PLDS.

Original 3-tier system

Prior to Release 4.1, VSP 4000 employed a three-tier licensing system:

- the Base Software License
- the Advanced License
- the Premier License

The Base Software License was free of charge and more advanced features could be purchased separately, if required. The following table shows the three tiers and the features they supported.

Table 43: Avaya Data Licensing Portal three-tier system

Base (Layer 2 features)	Advanced (Layer 3 features)	Premier (Layer 3 Virtualization and MACsec)
<ul style="list-style-type: none"> • Core Layer 2 switching, ACLs, policers, shapers, 802.1D/w/s, 802.1p/Q • MLT/LACP • SPB base functionality 	<ul style="list-style-type: none"> • IP routing features: <ul style="list-style-type: none"> - GRT IP routing - SPB IP shortcuts - SPB Inter-ISID routing - VRRP 	<ul style="list-style-type: none"> • Layer 3 virtualization features: <ul style="list-style-type: none"> - IP VRFs - SPB L3 VSNs with Static Routing - MACsec

Base (Layer 2 features)	Advanced (Layer 3 features)	Premier (Layer 3 Virtualization and MACsec)
<ul style="list-style-type: none"> • SPB L2 VSNs • SPB IEEE 802.1ag CFM 	<ul style="list-style-type: none"> - DHCP relay 	

License files in this three-tier system used the .dat extension.

PLDS 2-tier system

Beginning in Release 4.1, VSP 4000 uses PLDS as the license order, delivery and management tool. PLDS provides a two-tier framework: a Base Software License and a Premier License.

The Base Software License is free of charge with the purchase of VSP 4000 hardware. You can purchase a Premier License to unlock additional features. The following table shows the two tiers and the features they support.

Table 44: PLDS two-tier system

Base (Layer 2 features)	Premier
<ul style="list-style-type: none"> • Layer 2 Features <ul style="list-style-type: none"> - Core Layer 2 Switching, ACLs, Policers, Shapers - IEEE 802.1D/w/s, IEEE 802.1p/Q - MLT/LACP - SPB Base functionality - SPB Layer 2 VSNs (including Multicast) - SPB IEEE 802.1ag CFM - E-Tree/Private VLANs - <i>Transparent Port UNI</i> - Switch Clustering with virtual IST (SMLT with vIST) • IPv4 and IPv6 routing features: <ul style="list-style-type: none"> - GRT IP Routing - Static routing, RIP, OSPF v2/v3, BGP - VRRP v2/v3 - DHCP Relay - Configured Tunnels (6 in 4) - ISIS Accept Policies for IPv4 Routing - SPB IP shortcuts (IPv4 and IPv6) - SPB Inter-VSN Routing - Routed Switch Clustering with virtual IST (R-SMLT with vIST) 	<ul style="list-style-type: none"> • Layer 3 Virtualization features: <ul style="list-style-type: none"> - SPB Layer 3 VSNs (including Multicast) - IEEE 802.1AE MACsec

Base (Layer 2 features)	Premier
<ul style="list-style-type: none"> • IP Multicast features: <ul style="list-style-type: none"> - IGMP - MLD v1/v2 host mode - PIM SM/SSM - IP Multicast over Fabric Connect • Layer 3 Virtualization features: <ul style="list-style-type: none"> - IPv4 VRFs 	

PLDS license files use the `.xml` extension.

Upgrading to 4.1 or later

When you upgrade your VSP 4000 deployment to VOSS 4.1 or later, previously purchased and installed licenses continue to operate. You do not need to convert old license files.

VOSS 4.1 and later ignore previously installed Advanced licenses because features enabled by Advanced licenses are now part of the Base Software License.

The procedure to install and load licenses on a switch remains the same. Note that the PLDS license file type is `.xml` as opposed to the `.dat` extension that was used by the older licensing system. If you have both a `.dat` license file and a `.xml` license file in the `/intflash/` directory, the `.xml` file receives preference.

Avaya recommends that you leave existing Advanced license installations intact on the switch, so that there is no impact to licensed features in the unlikely event of a software downgrade to Release 4.0 or earlier.

For information about Avaya PLDS, see *Getting Started with Avaya PLDS for Avaya Networking Products, NN46199-300*.

For information and procedures about how to install licenses, see the following tasks:

- [License installation using ACLI](#) on page 150
- [License installation using EDM](#) on page 154

Chapter 19: License installation using ACLI

Install and manage a license file for Avaya Virtual Services Platform 4000 Series by using the Avaya command line interface (ACLI).

Installing a license file

Install a license file on Avaya Virtual Services Platform 4000 Series to enable licensed features.

Before you begin

- File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
- You must enable the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server depending on which protocol you use to download the license file to the device.
- Ensure that you have the correct license file with the base MAC address of Virtual Services Platform 4000 on which you need to install the license. Otherwise, the system does not unblock the licensed features. For more information about how to obtain a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

About this task

Note:

You can enable FTP or TFTP in the boot config flags, and then initiate an FTP or a TFTP session from your workstation to put the file on the server running on the VSP 4000.

Important:

The license filename stored on a device must meet the following requirements:

- Maximum of 63 alphanumeric characters
- No spaces or special characters allowed
- Underscore (_) is allowed
- The file extension ".xml" is required

If more than one valid .xml license file exists in the `/intflash/` directory, the switch uses the license with the highest capability.

Procedure

1. From a remote station, or PC, use FTP or TFTP to download the license file to the device, and store the license file in the `/intflash/` directory.
2. Enter Global Configuration mode:

```
enable
configure terminal
```

3. To load the license file, execute the following command:

```
load-license
```

Important:

If the loading fails, or if the switch restarts and cannot locate a license file in the specified location, the switch cannot unlock the licensed features and reverts to base functionality.

Example

Use FTP to transfer a license file from a PC to the internal flash on the device:

```
C:\Users\jsmith>ftp 192.0.2.16
Connected to 192.0.2.16 (192.0.2.16).
220 FTP server ready
Name (192.0.2.16:(none)): rwa
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put premier_macsec.xml /intflash/premier_macsec.xml
local: premier_macsec.xml remote: /intflash/premier_macsec.xml
227 Entering Passive Mode (192,0,2,16,4,2)
150 Opening BINARY mode data connection
226 Transfer complete
101 bytes sent in 2.7e-05 secs (3740.74 Kbytes/sec)
ftp>
```

Log in to the device and load the license. The following example shows a successful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1 [06/12/15 15:59:57.636:UTC] 0x000005bc 00000000 GlobalRouter SW INFO
License Successfully Loaded From </intflash/premier_macsec.xml> License Type -- PREMIER
+MACSEC
```

The following example shows an unsuccessful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1 [06/12/15 15:58:48.376:UTC] 0x000006b9 00000000 GlobalRouter SW
INFO Invalid license file /intflash/license_VSP_4000_example.xml HostId is not Valid

CP1 [06/12/15 15:58:48.379:UTC] 0x000005c4 00000000 GlobalRouter SW INFO No Valid
License found.
```

Variable definitions

Use the data in the following table to help you install a license with the `copy` command.

Table 45: Variable definitions

Variable	Value
<a.b.c.d>	Specifies the IPv4 or IPv6 address of the TFTP server from which to copy the license file.
<file>	Specifies the name of the license file when copied to the flash. The destination file name must meet the following requirements: <ul style="list-style-type: none"> • Maximum of 63 alphanumeric characters • No spaces or special characters allowed • Underscore (<code>_</code>) is allowed • The file extension ".xml" is required
<srcfile>	Specifies the name of the license file on the TFTP server. For example, premier.xml or premier_macsec.xml.

Showing a license file

Display the existing software licenses on your device.

Procedure

Show the existing software licenses on your device:

```
show license
```

Example

For no license:

```
Switch:1>show license
No license file is loaded.
Basic feature set is available without license.

*****
Features requiring a Premier license:
  - Layer 3 VSNs
  - MACsec
  - Fabric Extend
```

The output for the "show license" cli command for legacy licenses will show non-zero values for MD5 of Key and MD5 of file:

```
Switch:1>show license

License file name      : /intflash/premier.dat
```

```

License Type      :    PREMIER
MD5 of Key       :    7ce34d20 0caf0074 6657d928 1b4a0a18
MD5 of File      :    9e0e5a4c 4855efb1 90909c11 bb870d84
Generation Time  :    2015/08/12 01:53:39
Expiration Time  :
Base Mac Addr   :    b4:47:5e:37:9a:00
flags           :    0x00000001 SINGLE
memo            :

```

```

*****
Features requiring a Premier license:
- Layer 3 VSNS
- MACsec
- Fabric Extend

```

The output for the "show license" cli command for PLDS licenses will show all zeroes for MD5 of Key and MD5 of file:

```
Switch:1>show license
```

```

License file name :    /intflash/license.xml
License Type      :    PREMIER
MD5 of Key       :    00000000 00000000 00000000 00000000
MD5 of File      :    00000000 00000000 00000000 00000000
Generation Time  :    /13/03 EDT 2016
Expiration Time  :
Base Mac Addr   :    6c:a8:49:70:89:00
flags           :    0x00000001 SINGLE
memo            :

```

```

*****
Features requiring a Premier license:
- Layer 3 VSNS
- MACsec
- Fabric Extend

```

Chapter 20: License installation using EDM

Install and manage a license file for Avaya Virtual Services Platform 4000 Series by using Enterprise Device Manager (EDM).

Installing a license file

Install a license file on Avaya Virtual Services Platform 4000 Series to enable licensed features.

Before you begin

- You must store the license file on a file server.
- Ensure that you have the correct license file with the base MAC address of the Virtual Services Platform 4000 on which you need to install the license. Otherwise, the system does not unblock the licensed features.

About this task

IPv4 and IPv6 addresses are supported.

Important:

The license filename stored on a device must meet the following requirements:

- Maximum of 63 alphanumeric characters
- No spaces or special characters allowed
- Underscore (`_`) is allowed
- The file extension `.xml` is required

If more than one valid `.xml` license file exists in the `/intflash/` directory, the switch uses the license with the highest capability.

If you purchased the license prior to the introduction of PLDS in VOSS 4.1, see [Transition to PLDS](#) on page 147.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **File System**.
3. Click the **Copy File** tab.

4. In the **Source** box, type the IP address of the file server where the license file is located and the name of the license file.
5. In the **Destination** box, type the file path as `/intflash/<name of license file>`, for example, `/intflash/premier.xml`.

The license file name must have a file extension of `.xml`.

6. Select **start**.
7. Click **Apply**.

The license file is copied to the flash of the device. The status of the file copy appears in the Result field.

8. In the navigation tree, open the following folders: **Configuration > Edit**.
9. Click **Chassis**.
10. Click the **System** tab.
11. In **ActionGroup1**, select **loadLicense**.
12. Click **Apply**.

! **Important:**

If the loading fails, the switch cannot unlock the licensed features and reverts to base functionality.

13. On the **System** tab, in **ActionGroup1**, select **saveRuntimeConfig**.
14. Click **Apply**.

Copy File field descriptions

Use the data in the following table to use the **Copy File** tab.

Name	Description
Source	Identifies the source file to copy. You must specify the full path and filename.
Destination	Identifies the device and the file name (optional) to which to copy the source file. You must specify the full path. Trace files are not a valid destination.
Action	Starts the copy process or stops the copy process.
Result	Specifies the result of the copy process: <ul style="list-style-type: none"> • none • inProgress • success • fail

Table continues...

Name	Description
	<ul style="list-style-type: none">• invalidSource• invalidDestination• outOfMemory• outOfSpace• fileNotFound

Chapter 21: NTP fundamentals

This section provides conceptual material on the Network Time Protocol (NTP). Review this content before you make changes to the NTP configuration

Overview

The Network Time Protocol (NTP) synchronizes the internal clocks of various network devices across large, diverse networks to universal standard time. NTP runs over the User Datagram Protocol (UDP), which in turn runs over IP. The NTP specification is documented in Request For Comments (RFC) 1305.

Every network device relies on an internal system clock to maintain accurate time. On local devices, the internal system clock is usually set by eye or by wristwatch to within a minute or two of the actual time and is rarely reset at regular intervals. Many local clocks are battery-backed devices that use room temperature clock oscillators that can drift as much as several seconds each day. NTP automatically adjusts the time of the devices so that they synchronize within a millisecond (ms) on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC).

The current implementation of NTP supports only unicast client mode. In this mode, the NTP client sends NTP time requests to other remote time servers in an asynchronous fashion. The NTP client collects four samples of time from each remote time server. A clock selection algorithm determines the best server among the selected samples based on stratum, delay, dispersion and the last updated time of the remote server. The real time clock (RTC) is adjusted to the selected sample from the chosen server.

NTP terms

A peer is a device that runs NTP software. However, this implementation of NTP refers to peers as remote time servers that provide time information to other time servers on the network and to the local NTP client. An NTP client refers to the local network device, Avaya Virtual Services Platform 4000 Series, that accepts time information from other remote time servers.

NTP system implementation model

NTP is based on a hierarchical model that consists of a local NTP client that runs on Virtual Services Platform 4000 and on remote time servers. The NTP client requests and receives time information from one or more remote time servers. The local NTP client reviews the time information

from all available time servers and synchronizes its internal clock to the time server whose time is most accurate. The NTP client does not forward time information to other devices that run NTP.

Two types of time servers exist in the NTP model: primary time servers and secondary time servers. A primary time server is directly synchronized to a primary reference source, usually a wire or radio clock that is synchronized to a radio station that provides a standard time service. The primary time server is the authoritative time source in the hierarchy, meaning that it is the one true time source to which the other NTP devices in the subnet synchronize their internal clocks.

A secondary time server uses a primary time server or one or more secondary time servers to synchronize its time, forming a synchronization subnet. A synchronization subnet is a self-organizing, hierarchical master-backup configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels.

The following figure shows NTP time servers forming a synchronization subnet.

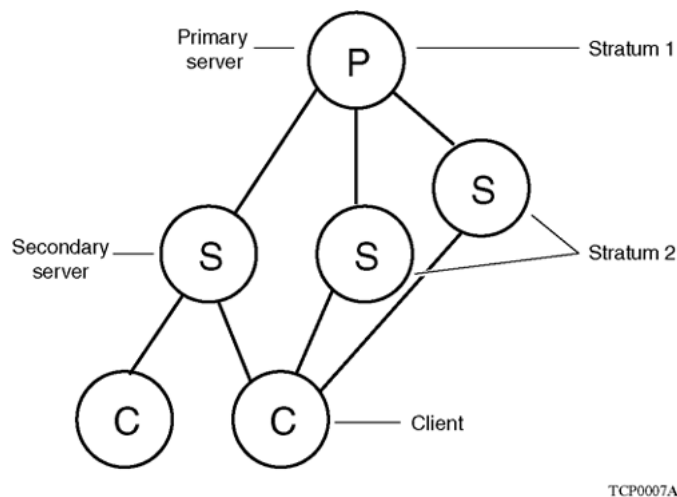


Figure 2: NTP time servers forming a synchronization subnet

In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary configuration to produce accurate and reliable time, even if one or more primary time servers or the path between them fails. This feature applies in a case in which all the primary servers on a partitioned subnet fail, but one or more backup primary servers continue to operate. If all of the primary time servers in the subnet fail, the remaining secondary servers synchronize among themselves.

Time distribution within a subnet

NTP distributes time through a hierarchy of primary and secondary servers, with each server adopting a stratum, see [Figure 2: NTP time servers forming a synchronization subnet](#) on page 158. A stratum defines how many NTP hops away a particular secondary time server is from an authoritative time source (primary time server) in the synchronization subnet. A stratum 1 time server is located at the top of the hierarchy and is directly attached to an external time source, typically a wire or radio clock; a stratum 2 time server receives its time through NTP from a stratum

1 time server; a stratum 3 time server receives its time through NTP from a stratum 2 time server, and so forth.

Each NTP client in the synchronization subnet chooses as its time source the server with the lowest stratum number with which it is configured to communicate through NTP. This strategy effectively builds a self-organizing tree of NTP speakers. The number of strata is limited to 15 to avoid long synchronization loops.

NTP avoids synchronizing to a remote time server with inaccurate time. NTP never synchronizes to a remote time server that is not itself synchronized. NTP compares the times reported by several remote time servers.

Synchronization

Unlike other time synchronization protocols, NTP does not attempt to synchronize the internal clocks of the remote time servers to each other. Rather, NTP synchronizes the clocks to universal standard time, using the best available time source and transmission paths to that time source.

NTP uses the following criteria to determine the best available time server:

- The time server with the lowest stratum.
- The time server closest in proximity to the primary time server (reduces network delays).
- The time server that offers the highest claimed precision.

NTP accesses several (at least three) servers at the lower stratum level because it can apply an agreement algorithm to detect a problem on the time source.

NTP modes of operation

NTP uses unicast client mode to enable time servers and NTP clients to communicate in the synchronization subnet. Virtual Services Platform 4000 supports only unicast client mode.

After you configure a set of remote time servers (peers), NTP creates a list that includes each time server IP address. The NTP client uses this list to determine the remote time servers to query for time information.

After the NTP client queries the remote time servers, the servers respond with various timestamps, along with information about their clocks, such as stratum, precision, and time reference, see [Figure 3: NTP time servers operating in unicast client mode](#) on page 160. The NTP client reviews the list of responses from all available servers and chooses one as the best available time source from which to synchronize its internal clock.

The following figure shows how NTP time servers operate in unicast mode.

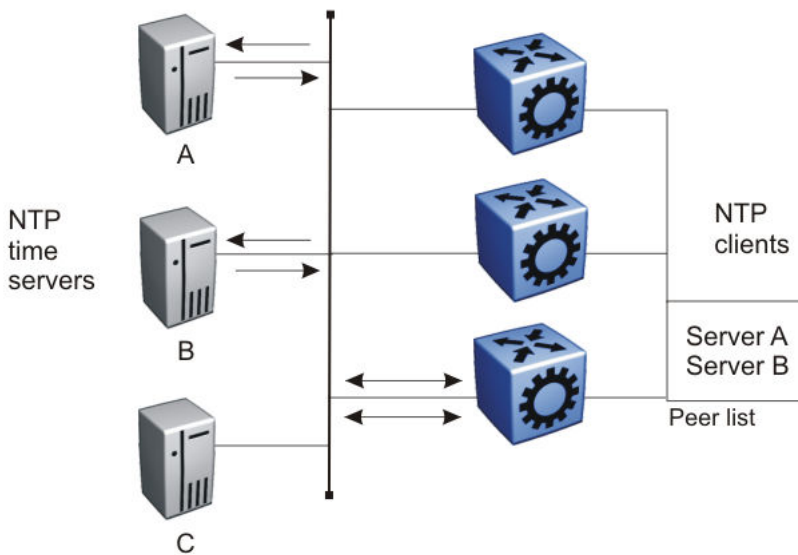


Figure 3: NTP time servers operating in unicast client mode

NTP authentication

You can authenticate time synchronization to ensure that the local time server obtains its time services only from known sources. NTP authentication adds a level of security to your NTP configuration. By default, network time synchronization is not authenticated.

If you select authentication, Virtual Services Platform 4000 uses the Message Digest 5 (MD5) algorithm or the Secure Hash Algorithm 1 (SHA1) algorithm to produce a message digest of the key. The message digest is created using the key and the message, but the key itself is not sent. Depending on which algorithm you select, the MD5 or SHA1 algorithm verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

To authenticate the message, the client authentication key must match that of the time server. Therefore, you must securely distribute the authentication key in advance (the client administrator must obtain the key from the server administrator and configure it on the client).

While a server can know many keys (identified by many key IDs) it is possible to declare only a subset of these as trusted. The time server uses this feature to share keys with a client that requires authenticated time and that trusts the server, but that is not trusted by the time server.

Chapter 22: NTP configuration using ACLI

This section describes how to configure the Network Time Protocol (NTP) using Avaya Command Line Interface (ACLI).

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on Avaya Virtual Services Platform 4000 Series and ensure that the NTP server is reachable through this interface. For instructions, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505.
- Ensure the Real Time Clock is present on the module.

 **Important:**

NTP server MD5 authentication or SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

This task flow shows the sequence of procedures you perform to configure NTP.

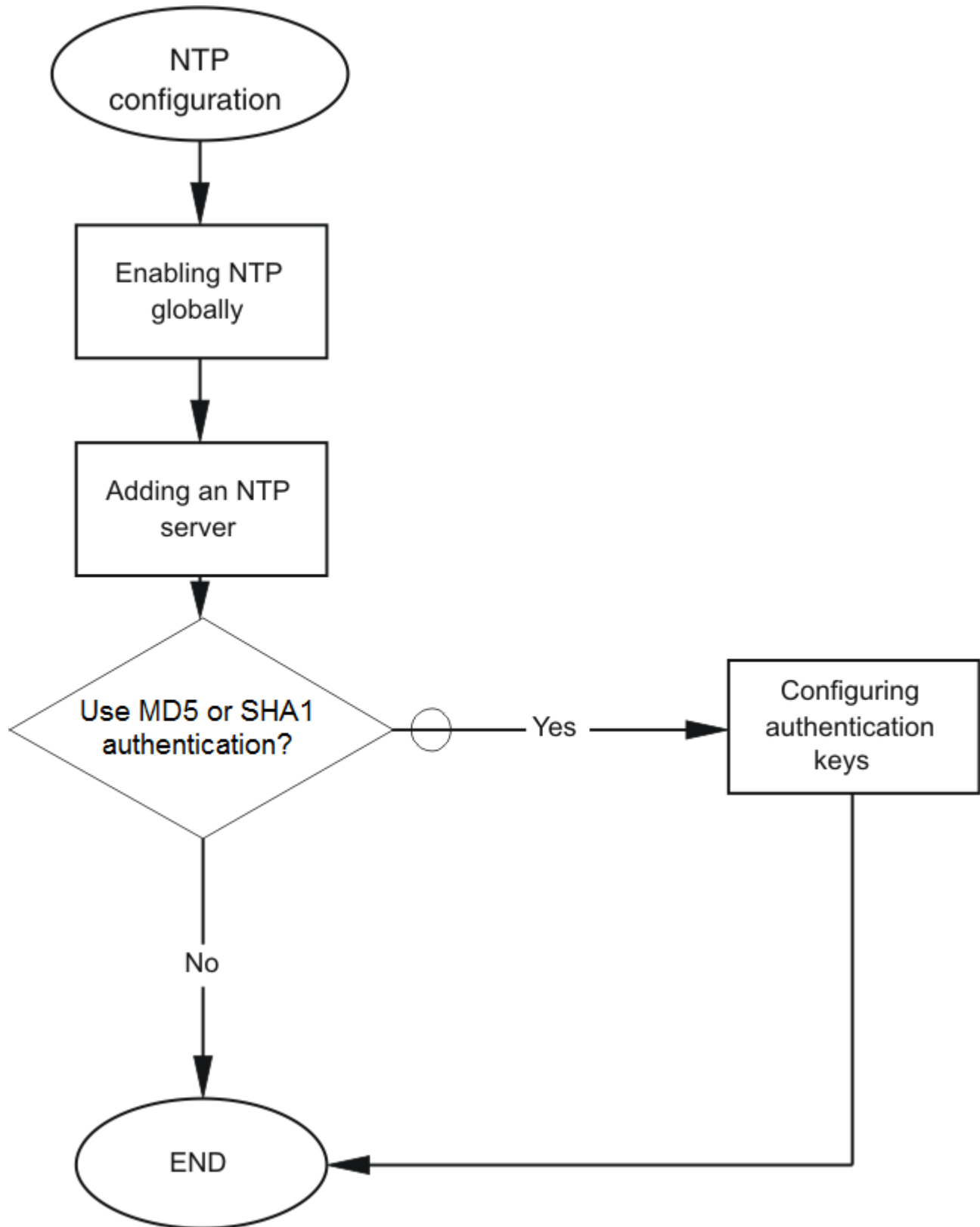


Figure 4: NTP configuration procedures

Related links

[Enabling NTP globally](#) on page 163

Enabling NTP globally

Enable NTP globally. Default values are in effect for most parameters. You can customize NTP by modifying parameters.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. **(Optional)** Set the time interval between NTP updates or leave it at the default of 15 minutes:

```
ntp interval <10-1440>
```

! **Important:**

If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

3. Enable NTP globally:

```
ntp
```

4. Create an authentication key:

```
ntp authentication-key <1-2147483647> WORD<0-20> type <md5|sha1>
```

Example

Specify the interval between NTP updates to 10 minutes, and then enable NTP globally.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp interval 10
Switch:1(config)#ntp
```

Create an authentication key.

```
Switch:1(config)#ntp authentication-key 1 test type sha1
```

Related links

[NTP configuration using ACLI](#) on page 161

[Variable definitions](#) on page 164

Variable definitions

Use the data in the following table to use the `ntp` command.

Variable	Value
authentication-key <1-2147483647> WORD<0–20>	<p>Creates an authentication key for MD5 or SHA1 authentication. To set this option to the default value, use the default operator with the command. The default configuration is to delete the authentication key.</p> <p>NTP server MD5 or SHA1 authentication does not support passwords (keys) that start with a special character or contain a space between characters.</p> <p><i>WORD</i><0–20> specifies the secret key.</p>
interval <10-1440>	<p>Specifies the time interval, in minutes, between successive NTP updates.</p> <ul style="list-style-type: none"> The interval is expressed as an integer in a range from 10–1440. The default value is 15. <p>If you changed the interval and then wanted to reset it back to the default, use the <code>default ntp interval</code> command.</p>
type <md5 sha1>	<p>Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.</p>

Related links

[Enabling NTP globally](#) on page 163

Adding an NTP server

About this task

Add an NTP server or modify existing NTP server parameters by performing this procedure. You can configure a maximum of 10 time servers.

Procedure

- Enter Global Configuration mode:


```
enable
configure terminal
```
- Add an NTP server:


```
ntp server <A.B.C.D>
```
- Configure additional options for the NTP server:

```
ntp server <A.B.C.D> [auth-enable] [authentication-key
<0-2147483647>] [source-ip WORD <0-46>]
```

4. Activate the NTP server:

```
ntp server <A.B.C.D> enable
```

Example

```
VSP-4850GTS-PWR+:> enable
VSP-4850GTS-PWR+:1 configure terminal
VSP-4850GTS-PWR+:1(config)# ntp server 192.0.2.187
```

Variable definitions

Use the data in the following table to use the `ntp server` command.

Variable	Value
server <A.B.C.D>	Specifies the IP address of the NTP server.
auth-enable	Activates MD5 or SHA1 authentication on this Network Time Protocol (NTP) server. Without this option, the NTP server will not have any authentication by default.
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 or SHA digest for the NTP server. The default authentication key is 0, which indicates disabled authentication.
source-ip WORD <0-46>	Specifies the source IP for the server. If you do not configure source-ip, by default, the source-ip entry is initialized to 0.0.0.0. The IP address specified can be any local interface.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.

Configuring authentication keys

About this task

Configure NTP authentication keys to use MD5 or SHA1 authentication.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create an authentication key:

```
ntp authentication-key <1-2147483647> WORD<0-8> [type <md5|sha1>]
```

3. Enable MD5 authentication for the server:

```
ntp server <A.B.C.D> auth-enable
```

4. Assign an authentication key to the server:

```
ntp server <A.B.C.D> authentication-key <0-2147483647>
```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Create the authentication key:

```
Switch:1#(config)# ntp authentication-key 5 test type md5
```

Enable MD5 authentication for the NTP server:

```
Switch:1#(config)# ntp server 192.0.2.187 auth-enable
```

Assign an authentication key to the server:

```
Switch:1#(config)# ntp server 192.0.2.187 authentication-key 5
```

Variable definitions

Use the data in the following table to use the `ntp` and `ntp server` commands.

Table 46: Variable definitions

Variable	Value
A.B.C.D	Specifies the IP address of the server.
auth-enable	Activates MD5 or SHA1 authentication on this NTP server. The default is no authentication. To set this option to the default value, use the default operator with the command.
authentication-key <1-2147483647> WORD<0-20>	Creates an authentication key for MD5 or SHA1 authentication. To set this option to the default value, use the default operator with the command. The default configuration is to delete the authentication key.
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 or SHA1 digest for the NTP server. The value range is an integer from 0–2147483647. The default value is 0, which indicates disabled authentication. To set this option to the default value, use the default operator with the command.
type <md5 sha1>	Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

Chapter 23: NTP configuration using EDM

This section describes how to configure the Network Time Protocol (NTP) using Enterprise Device Manager (EDM).

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the Avaya Virtual Services Platform 4000 Series and ensure that the NTP server is reachable through this interface. For instructions, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505.
- Ensure the Real Time Clock is present on the module.

 **Important:**

NTP server MD5 authentication or SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

This task flow shows you the sequence of procedures you perform to configure NTP.

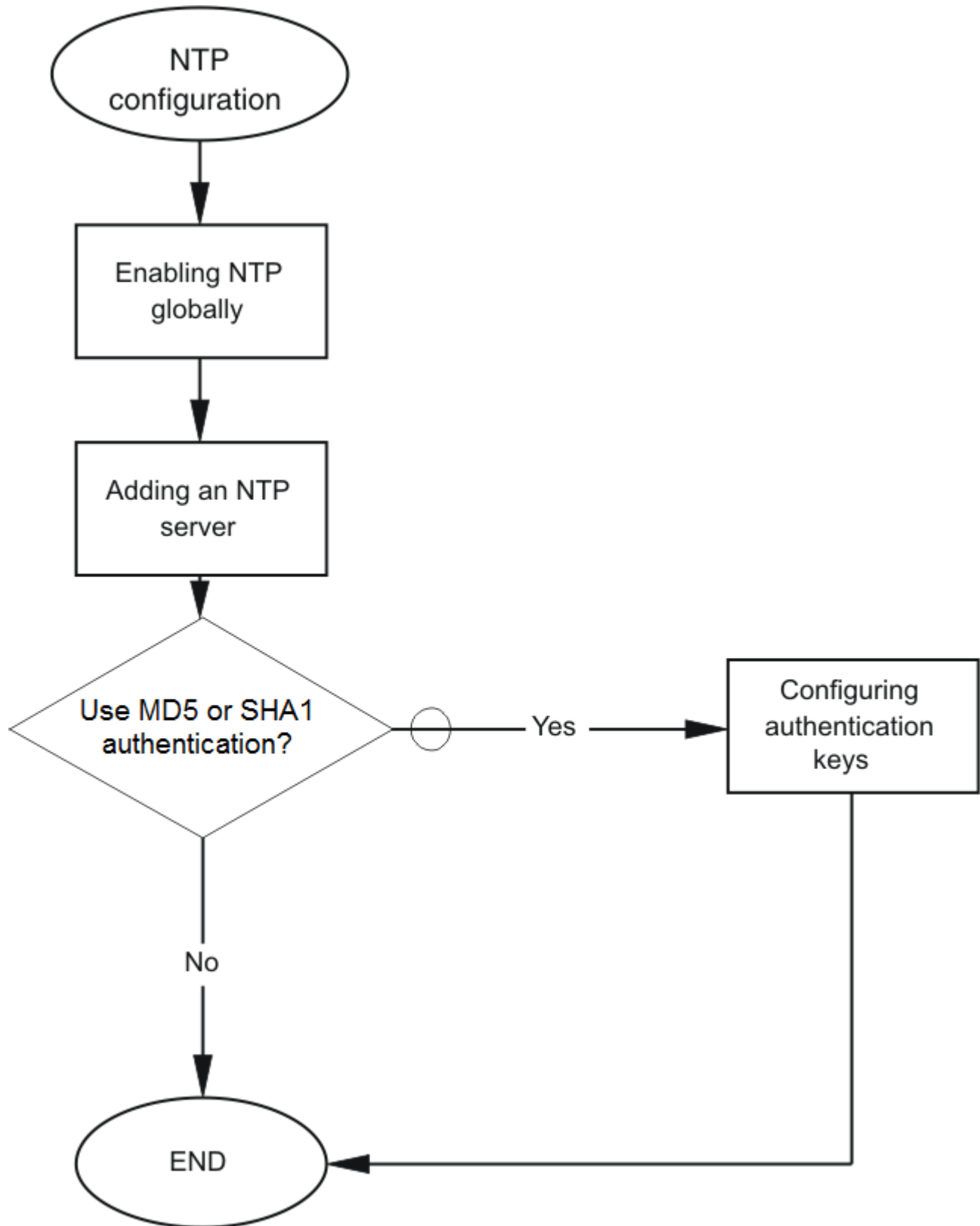


Figure 5: NTP configuration procedures

Enabling NTP globally

About this task


Enable NTP globally. Default values are in effect for most parameters. You can customize NTP by modifying parameters.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **NTP**.
3. Click the **Globals** tab.
4. Select the **Enable** check box.
5. Click **Apply**.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
Enable	Activates (true) or disables (false) NTP. By default, NTP is disabled.
Interval	<p>Specifies the time interval (10–1440 minutes) between successive NTP updates. The default interval is 15 minutes.</p> <p> Important: If NTP is already activated, this configuration does not take effect until you disable NTP, and then reenable it.</p>

Adding an NTP server

About this task

Add a remote NTP server to the configuration by specifying its IP address. NTP adds this IP address to a list of servers, which the local NTP client uses to query remote time servers for time information. The list of qualified servers called to is a peer list.

You can configure a maximum of 10 time servers.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **NTP**.
3. Click the **Server** tab.

4. Click **Insert**.
5. Specify the IP address of the NTP server.
6. Click **Insert**.

The IP address of the NTP server that you configured appears on the Server tab.

Server field descriptions

Use the data in the following table to use the **Server** tab.

Name	Description
ServerAddress	Specifies the IP address of the remote NTP server.
Enable	Activates or disables the remote NTP server. The default is enabled.
Authentication	Activates or disables MD5 or SHA1 authentication on this NTP server. MD5 or SHA1 produces a message digest of the key. MD5 or SHA1 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The default is no authentication.
KeyId	Specifies the key ID used to generate the MD5 or SHA1 digest for this NTP server. You must specify a number between 1–214743647. The default is 0, which indicates that authentication is disabled.
SourceIpAddress	Specifies the source IPv4 address for the server. If you do not configure source-ip, by default, the source-ip entry is initialized to 0.0.0.0. The IP address specified can be any local interface.
AccessAttempts	Specifies the number of NTP requests sent to this NTP server.
AccessSuccess	Specifies the number of times this NTP server updated the time.
AccessFailure	Specifies the number of times the client rejected this NTP server while it attempted to update the time.
Stratum	This variable is the stratum of the server.
Version	This variable is the NTP version of the server.
RootDelay	This variable is the root delay of the server.
Precision	This variable is the NTP precision of the server in seconds.
Reachable	This variable is the NTP reach ability of the server.
Synchronized	This variable is the status of synchronization with the server.

Configuring authentication keys

About this task


Assign an NTP key to use MD5 or SHA1 authentication on the server.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Edit**.
2. Click **NTP**.
3. Click the **Key** tab.
4. Click **Insert**.
5. Specify the secret key in the **KeySecret** field.
6. Select md5 or sha1 in the **KeyType** field.
7. Click **Insert**.

Key field descriptions

Use the data in the following table to use the **Key** tab.

Name	Description
KeyId	This field is the key ID that generates the MD5 or SHA1 digest. You must specify a value between 1–214743647. The default value is 1, which indicates that authentication is disabled.
KeySecret	This field is the MD5 or SHA1 key that generates the MD5 or SHA1 digest. You must specify an alphanumeric string between 0–20  Important: You cannot specify the number sign (#) as a value in the KeySecret field. The NTP server interprets the # as the beginning of a comment and truncates all text entered after the #.
KeyType	This field specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

Chapter 24: Secure Shell fundamentals

Secure Shell (SSH) is a client and server protocol that specifies the way to conduct secure communications over a network. The traffic these utilities generate is not encrypted when using other methods of remote access such as Telnet or FTP. Anyone that can see the network traffic can see all data, including passwords and user names. Secure Shell can replace Telnet and other remote login utilities. Secure File Transfer Protocol (SFTP) can replace FTP with an encrypted alternative.

*** Note:**

If both SSH and SFTP are concurrently active, you have the ability to disable SFTP while allowing SSH to remain active. For more information, see [Disabling SFTP without disabling SSH](#) on page 196.

VOSS 5.0 introduces Secure CoPy protocol (SCP) which is a secure file transfer protocol. SCP is used for securely transferring files between a local host and a remote host. SCP is in off state by default, but you can turn it on when you enable SSH using the `boot config flags` command in the global config mode. VOSS supports SCP only as an SCP server, which means that clients can send files to the VOSS switch or can request files from the switch. Secure CoPy (SCP) can replace FTP with an encrypted alternative.

Secure Shell supports a variety of the different public and private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key encrypts all traffic between the client and the server. The VSP switch supports Secure Shell version 2 (SSHv2).

*** Note:**

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the `.ssh` directory and generate new keys for SSH. For more information about supported software, see *Release Notes for VSP Operating System Software*, NN47227-401.

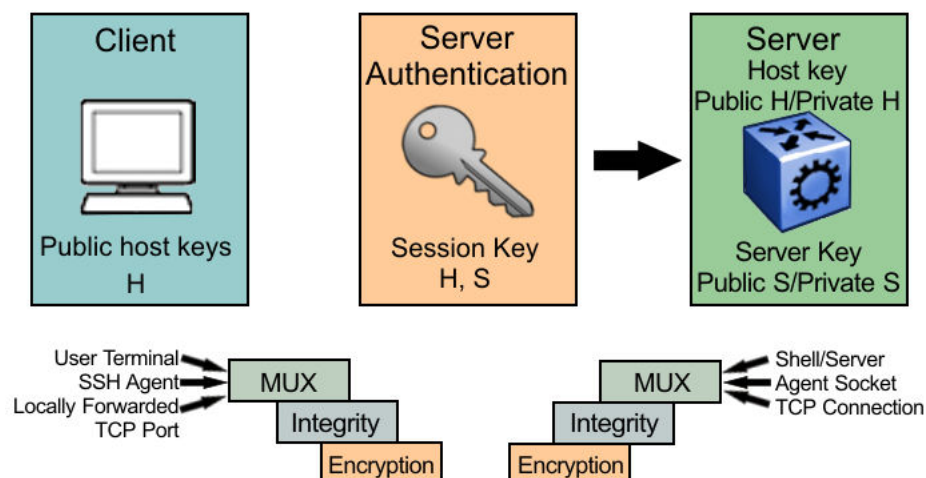


Figure 6: Overview of the SSH protocol

By using a combination of host, server, and session keys, the SSHv2 protocol can provide strong authentication and secure communication over an insecure network, offering protection from the following security risks:

- IP spoofing
- IP source routing
- Domain name server (DNS) spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping and password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

The SSH secure channel of communication does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

With the SSH server in the VSP switch, you can use an SSH client to make a secure connection to the VSP switch and work with commercially available SSH clients. For more information about supported clients, see [Table 48: Third-party SSH and SCP client software](#) on page 180. The VSP switch also supports outbound connections to remote SSH servers to provide complete inbound and outbound secure access.

Security features

The SSHv2 protocol supports the following security features:

- Authentication. This feature determines, in a reliable way, an SSHv2 client. During the log on process, the SSHv2 client is queried for a digital proof of identity.

Supported authentications with the switch as a server for SSHv2, are: RSA, DSA, and passwords. Supported authentications with the switch as a client for SSHv2, are: DSA and passwords. The VSP switch does not support RSA when the switch acts as a client.

When the VSP switch acts as an SSH server the VSP switch allows up to four sessions at a time. However, only one SSH public key encryption per access level is allowed at a time. For instance, if multiple SSH public key encryption clients have to connect to the VSP server with

the same access level, such as rwa then the clients must connect to the server one-by-one as the VSP only supports one public key per access level.

- Encryption. The SSHv2 server uses encryption algorithms to scramble data and render it unintelligible except to the receiver.

Supported encryption and ciphers are: 3DES, AES128-cbc, AES192-cbc, AES256-cbc, AES128-ctr, AES192-ctr, AES256-ctr, rijndael128-cbc, rijndael 192-cbc, aeadAes-128Gcm, aeadAes-256Gcm, blowfish-cbc, secure hash algorithm 1 (SHA-1) and SHA-2.

- Integrity. This feature guarantees that the data transmits from the sender to the receiver without alterations. If a third party captures and modifies the traffic, the SSHv2 server detects this alteration.

SSHv2 considerations using EDM

You must use the ACLI to initially configure SSHv2. You can use Enterprise Device Manager (EDM) to change the SSHv2 configuration parameters. However, Avaya recommends that you use ACLI. Avaya also recommends that you use the console port to configure the SSHv2 parameters.

Important:

Do not enable SSHv2 secure mode using Configuration and Orchestration Manager (COM). If you enable SSHv2 secure mode, then the system disables Simple Network Management Protocol (SNMP). This locks you out of a COM session. Enable SSH secure mode using ACLI or EDM.

SSHv2 secure mode is different from enhanced secure mode and hsecure. SSHv2 secure mode disables unsecure management protocols on the device such as FTP, rlogin, SNMP, telnet, and TFTP. SSHv2 secure mode is enabled through the `ssh secure` command.

When you enable SSHv2 secure mode, the system disables FTP, rlogin, SNMPv1, SNMPv2, SNMPv3, telnet and TFTP. After SSHv2 secure mode is enabled, you can choose to enable individual non-secure protocols. However, after you save the configuration and restart the system, the non-secure protocol is again disabled, even though it is shown as enabled in the configuration file. After you enable SSHv2 secure mode, you cannot enable non-secure protocols by disabling SSHv2 secure mode.

You can disable block-snmpp after you enable SSHv2 secure mode, and you can connect again using COM.

Interoperability

The VSP SSHv2 client can operate with the following SSHv2 servers:

- Another VSP 4000
- ERS 8600/8800
- Linux running Open SSH
- VSP 7000
- VSP 7200
- VSP 9000

Outbound connections

The SSHv2 client supports SSHv2 DSA public key authentication and password authentication.

*** Note:**

You must enable SSH globally before you can generate SSH DSA user keys.

The SSHv2 client is a secure replacement for outbound Telnet. Password authentication is the easiest way to use the SSHv2 client feature.

Instead of password authentication, you can use DSA public key authentication between the VSP SSHv2 client and an SSHv2 server. Before you can perform a public key authentication, you must generate the key pair files and distribute the key files to all the SSHv2 server systems. Because passphrase encrypts and further protects the key files, you must provide a passphrase to decrypt the key files as part of the DSA authentication.

To attempt public key authentication, the SSH client looks for the associated DSA key pair files in the /intflash/.ssh directory. If no DSA key pair files are found, the SSHv2 client automatically prompts you for password authentication. If the SSHv2 client succeeds with the authentication, then a new secured SSHv2 session is established to the remote SSHv2 server. For more information, see [Table 49: DSA authentication access level and file name](#) on page 181.

! Important:

If you configure the DSA user key with a passphrase but you do not supply the correct passphrase when you try to make the SSH connection, then the system defaults back to the password authentication. If the SSH client succeeds with the authentication, then a new secured SSH session is established to the remote SSHv2 server.

SSH version 2

The SSH version 2 (SSHv2) protocol is a complete rewrite of the SSHv1 protocol. In SSHv2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

The SSH Transport Layer manages the server authentication and provides the initial connection between the client and the server. Once the connection is established, the Transport Layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

The SSH Authentication Protocol runs on top of the SSH Transport Layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

The SSH Connection Protocol runs on top of the SSH Transport Layer and user authentication protocols. SSH-CONN provides interactive logon sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

The following figure shows the three layers of the SSHv2 protocol.

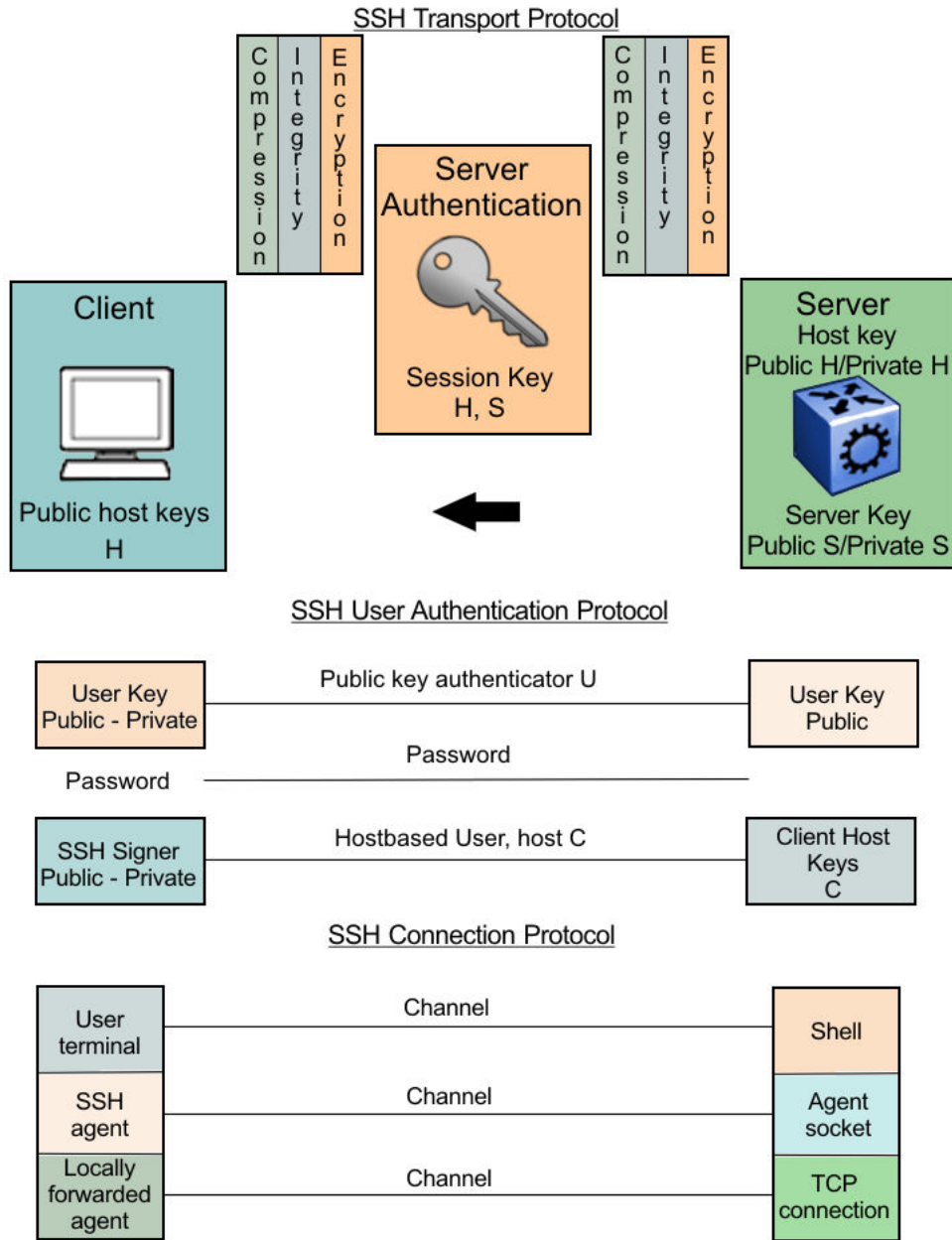


Figure 7: Separate SSH version 2 protocols

The modular approach of SSHv2 improves on the security, performance, and portability of the SSHv1 protocol.

! Important:

The SSHv1 and SSHv2 protocols are not compatible. The VSP switch does not support SSHv1.

User ID log of an SSH session established by SCP client

Avaya Virtual Services Platform 8200 logs the user ID of an SSH session initiated by the SCP client. If an SCP client establishes an SSH session, the message appears in the following format:

```
CP1 [08/06/15 09:43:42.230:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH user authentication succeeded for user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:42.232:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH SCP session start by user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:44.020:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SCP session closed by user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:44.021:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH session closed by user rwa on host 10.68.231.194
```

- rwa is the user name.

User ID log of an SSHv2 session established by SFTP

Virtual Services Platform 4000 logs the user ID of an SSH session initiated by SFTP. If an SFTP establishes an SSH session, the message appears in the following format:

```
CP1 [08/06/15 09:45:32.903:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH user authentication succeeded for user rwa on host 10.68.231.194
CP1 [08/06/15 09:45:32.905:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SFTP session start: user rwa on host 10.68.231.194
CP1 [08/06/15 09:45:46.775:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SFTP session closed by user rwa on host 10.68.231.194
CP1 [08/06/15 09:45:46.776:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH SFTP session end: user rwa on host 10.68.231.194
CP1 [08/06/15 09:45:46.776:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH session closed by server for user rwa on host 10.68.231.194
```

- rwa is the user name.

User key files

Generating keys requires that you have free space on the flash. A typical configuration requires less than 2 kbyte of free space. Before you generate a key, verify that you have sufficient space on the flash, using the `dir` command. If the flash is full when you attempt to generate a key, an error message appears and the key is not generated. You must delete some unused files and regenerate the key.

If you remove only the public keys, enabling the SSH does not create new public keys.

SSHv2 password authentication uses the same login and password authentication mechanism as Telnet. SSHv2 client also supports DSA public key authentication compatible with VSP 4000 SSH server and Linux SSH server for SSHv2.

If VSP 4000 is the client, use the following table to locate the DSA user key files for DSA authentication for user access level `rwa`.

Table 47: DSA user key files

SSH server	SSH client side	SSH server side
VSP 4000	Private and public keys by access level: <ul style="list-style-type: none"> • rwa—/intflash/.ssh/id_dsa_rwa (private key), /intflash/.ssh/id_dsa_rwa.pub (public key) • rw—/intflash/.ssh/id_dsa_rw (private key), /intflash/.ssh/id_dsa_rw.pub (public key) • ro—/intflash/.ssh/id_dsa_ro (private key), /intflash/.ssh/id_dsa_ro.pub (public key) • rwl1—/intflash/.ssh/id_dsa_rwl1 (private key), /intflash/.ssh/id_dsa_rwl1.pub (public key) • rwl2—/intflash/.ssh/id_dsa_rwl2 (private key), /intflash/.ssh/id_dsa_rwl2.pub (public key) • rwl3—/intflash/.ssh/id_dsa_rwl3 (private key), /intflash/.ssh/id_dsa_rwl3.pub (public key) 	Public keys on the server side based on access level: <ul style="list-style-type: none"> • rwa—/intflash/.ssh/dsa_key_rwa (public key) • rw—/intflash/.ssh/dsa_key_rw (public key) • ro—/intflash/.ssh/dsa_key_ro (public key) • rwl1—/intflash/.ssh/dsa_key_rwl1 (public key) • rwl2—/intflash/.ssh/dsa_key_rwl2 (public key) • rwl3—/intflash/.ssh/dsa_key_rwl3 (public key)
Avaya Virtual Services Platform 8000 Series with enhanced secure mode enabled	Private and public keys by access role level: <ul style="list-style-type: none"> • administrator—/intflash/.ssh/id_dsa_admin (private key), /intflash/.ssh/id_dsa_admin.pub (public key) • operator —/intflash/.ssh/id_dsa_operator (private key), /intflash/.ssh/id_dsa_operator.pub (public key) • security —/intflash/.ssh/id_dsa_security (private key), /intflash/.ssh/id_dsa_security.pub (public key) • auditor —/intflash/.ssh/id_dsa_auditor (private key), /intflash/.ssh/id_dsa_auditor.pub (public key) 	Public keys on the server side based on access level: <ul style="list-style-type: none"> • administrator—/intflash/.ssh/dsa_key_admin (public key) • operator—/intflash/.ssh/dsa_key_operator (public key) • security—/intflash/.ssh/dsa_key_security (public key) • privilege—/intflash/.ssh/dsa_key_priv (public key) • auditor—/intflash/.ssh/dsa_key_auditor (public key)

Table continues...

SSH server	SSH client side	SSH server side
	<ul style="list-style-type: none"> • privilege —/intflash/.ssh/id_dsa_priv (private key), /intflash/.ssh/id_dsa_priv.pub (public key) 	
Linux with Open SSHv2	~/.ssh/id_dsa (private key) file permission 400 ~/.ssh/id_dsa.pub (public key) file permission 644	~/.ssh/authorized_keys (public key) file
ERS 8600/8800	—	/flash/.ssh/dsa_key_rwa (public key)

When you attempt to make an SSHv2 connection from the VSP 4000, the SSHv2 client looks in its own internal flash for the public key pair files. If the key files exist, the SSHv2 client prompts you for the passphrase to decrypt the key files. If the passphrase is correct, the SSHv2 client initiates the DSA key authentication to the remote SSHv2 server. The SSHv2 client looks for the login user access level public key file on the SSHv2 server to process and validate the public key authentication. If the DSA authentication is successful, then the SSHv2 session is established.

If no matching user key pair files exist on the client side when initiating the SSHv2 session, or if the DSA authentication fails, you are automatically prompted for a password to attempt password authentication.

If the remote SSHv2 server is a Linux system which is based on Open SSHv2 implementation, the server looks for the login user public key file ~/.ssh/authorized_keys by default for DSA authentication. For Linux SSHv2 client, the user DSA key pair files are located in the user home directory as ~/.ssh/id_dsa and ~/.ssh/id_dsa.pub.

Block SNMP

The boot flag setting for block-snmpp (`boot config flags block-snmpp`) and the runtime configuration of SSH secure (`ssh secure`) each modify the block-snmpp boot flag. If you enable SSH secure mode, the system automatically sets the block-snmpp boot flag to true; the change takes effect immediately. After enabling SSH in secure mode, you can manually change the block-snmpp flag to false to allow both SSH and SNMP access.

Important:

The block flag setting for block-snmpp blocks Simple Network Management Protocol (SNMP)v1, SNMPv2, and SNMPv3.

SCP command

Avaya recommends that you use short file names with the Secure CoPy (SCP) command. The entire SCP command, including all options, user names, and file names must not exceed 80 characters. Avaya supports incoming SCP connections to the device but does not support outgoing connections using an SCP client from the device.

Third-party SSHv2 and SCP client software

The following table describes the third-party SSHv2 and SCP client software that has been tested but is not included with this release.

Table 48: Third-party SSH and SCP client software

Client	Secure Shell (SSH)	Secure Copy (SCP)
Tera Term Pro with TTSSH extension MS Windows	<ul style="list-style-type: none"> • Supports SSHv2. • Authentication: <ul style="list-style-type: none"> - RSA is supported when the switch acts as a server. The VSP switch does not support RSA as a client. - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys. 	Client distribution does not include SCP client and does not support WinSCP Client.
Secure Shell Client MS Windows	<ul style="list-style-type: none"> • Supports SSHv2 client. • Authentication <ul style="list-style-type: none"> - DSA - Password • Provides a keygen tool. • It creates a DSA key in SSHv2 format. • Virtual Services Platform 4000 generates a log message stating that a DSA key has been generated. 	Client distribution includes an SCP client that is not compatible with Virtual Services Platform 4000.
OpenSSH Unix Solaris 2.5 / 2.6	<ul style="list-style-type: none"> • Supports SSHv2 clients. • Authentication: <ul style="list-style-type: none"> - RSA is supported when the switch acts as a server. The VSP switch does not support RSA as a client. - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys. 	Client distribution includes an SCP client that is supported on Virtual Services Platform 4000.
WinSCP	N/A	This SCP client is unsupported on Virtual Services Platform 4000.

VSP switch as client

The VSP switch acting as the SSHv2 client generates a DSA public and private server key pair. The public part of the key for DSA is stored in the following location:

```
/intflash/.ssh/dsa_key_rwa
```

The public part of the key must be copied to the SSH server and be named according to the server's naming requirement.

If the server is a VSP device, please consult [Table 49: DSA authentication access level and file name](#) on page 181 for proper naming convention.

If a DSA key pair does not exist, you can generate the DSA key pair using the `ssh dsa-user-key [WORD<1-15>] [size <1024-2048>]` command.

You need to copy the DSA public key to the SSHv2 server that you connect to using the VSP as a client. RSA is not supported when using the VSP switch as a client, but you can use RSA when the VSP switch is acting as the server.

VSP switch as server

After you install one of the SSHv2 clients you must generate a client and server key using the RSA or DSA algorithms.

To authenticate an SSHv2 client using DSA, the administrator must copy the public part of the client DSA key to /intflash/.ssh directory on the VSP modular switch that is acting as the SSHv2 server. The file that is copied over to the SSHv2 server must be named according to [Table 49: DSA authentication access level and file name](#) on page 181.

DSA authentication access level and file name

The following table lists the access levels and file names you must use to store the SSHv2 client authentication information using DSA, onto the VSP 4000 system acting as the SSHv2 server.

Table 49: DSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in non IETF and IETF format with enhanced secure mode disabled Note: * The VSP switch supports IETF and non-IETF for DSA.	RWA	/intflash/.ssh/dsa_key_rwa
	RW	/intflash/.ssh/dsa_key_rw
	RO	/intflash/.ssh/dsa_key_ro
	L3	/intflash/.ssh/dsa_key_rwl3
	L2	/intflash/.ssh/dsa_key_rwl2
	L1	/intflash/.ssh/dsa_key_rwl1
Client key in enhanced secure mode	administrator	/intflash/.ssh/dsa_key_admin
	operator	/intflash/.ssh/dsa_key_operator
	security	/intflash/.ssh/dsa_key_security
	privilege	/intflash/.ssh/dsa_key_priv
	auditor	/intflash/.ssh/dsa_key_auditor

Virtual Services Platform 4000 generates an RSA public and private server key pair. The public part of the key for RSA is stored in /intflash/.ssh/ssh_key_rsa_pub.key. If an RSA key pair does not exist,

then Virtual Services Platform 4000 automatically generates one when you enable the SSH server. To authenticate a client using RSA, the administrator must copy the public part of the client RSA key to Virtual Services Platform 4000.

RSA authentication access level and file name

The following table lists the access levels and file names you can use for storing the SSH client authentication information using RSA.

Table 50: RSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in IETF format with enhanced secure mode disabled.	RWA	/flash/.ssh/rsa_key_rwa
	RW	/flash/.ssh/rsa_key_rw
	RO	/flash/.ssh/rsa_key_ro
	L3	/flash/.ssh/rsa_key_rwl3
	L2	/flash/.ssh/rsa_key_rwl2
	L1	/flash/.ssh/rsa_key_rwl1
Client key with enhanced secure mode enabled	administrator	/intflash/.ssh/rsa_key_admin
	operator	/intflash/.ssh/rsa_key_operator
	security	/intflash/.ssh/rsa_key_security
	privilege	/intflash/.ssh/rsa_key_priv
	auditor	/intflash/.ssh/rsa_key_auditor

SSL certificates

TLS server generates a new self-signed certificate on boot and uses that by default. The self-signed certificate is available in `/.intflash/.cert/.ssl`. You can choose to use an online or offline CA signed certificate which will take precedence over the self-signed one.

* Note:

Older release certificates from folder `/.intflash/.ssh/` are not used.

The system does not confirm if the certificate is still valid. If no certificate exists, then the system generates a default certificate (host.cert and also the key file, host.key) with a validity period of 365 days.

If you need to use your own SSL certificate, you can upload the certificate and key files to the `/.intflash/.cert/.ssl` directory, and then rename the files to host.cert and host.key. Restart the system and the new certificate will be loaded during the boot-up process. Alternatively, you can use the `ssl certificate reset` command to install an existing certificate without a system reboot.

You can also use the `ssl certificate [validity-period-in-days <30-3650>]` command to install a new certificate and optionally, define an expiration date. You do not need to restart the system after you use this command.

The system does not validate the expiration date on the certificate and performs no action after the certificate expires. To confirm the expiration date, you must use Microsoft Internet Explorer or Mozilla Firefox to view the certificate. If you cannot connect to the switch using HTTPS and the web

portal displays a message of invalid certificate, that is an indication that the certificate on the switch is expired. You can replace the host.cert and host.key files with new files generated off the switch, or you can use the procedure [Managing an SSL certificate](#) on page 195 to generate a new certificate on the switch with a specific validity period.

The default certificate key length for a certificate generated on the switch is 2,048 bits.

SSH rekeying

SSH rekeying is an SSHv2 feature that allows the SSH server/client to force a key exchange between server and client, while changing the encryption and integrity keys. When you enable SSH rekeying, key exchanges occur after a pre-determined time interval or after the data transmitted in the session reaches the data-limit threshold. The default time-interval is 1 hour and the default data-limit is 1 GB. You can configure these values using the `ssh rekey` command.

SSH rekey is optional. You can enable SSH rekey only when SSH is enabled globally. Most SSH clients and servers do not provide a rekey mechanism, do not enable SSH rekey in such cases.

*** Note:**

You cannot enable SSH rekey selectively for either SSH client or server, it is enabled both on the SSH client and server together.

Chapter 25: Secure Shell configuration using ACLI

Use Secure Shell version 2 (SSHv2) to enable secure communications support over a network for authentication, encryption, and network Integrity.

Before you begin

- Disable the sshd daemon. All SSHv2 commands, except enable, require that you disable the sshd daemon.
- Set the user access level to read/write/all community strings.
- Disable all nonsecure access services. Avaya recommends that you disable the following services: Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Telnet, and rlogin. For more information about disabling access services, see [Enabling remote access services](#) on page 59.
- Avaya recommends that you use the console port to configure the SSHv2 parameters.

For information about downloading and enabling security encryption, see [Downloading software from the Avaya support site](#) on page 201.

Enabling the SSH server

Enable the SSHv2 server to provide secure communications for accessing the switch.

Before you begin

To enable SSH, ensure to enable rsa-auth or dsa-auth, or both.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable the SSHv2 server:

```
boot config flags sshd
```

3. Save the configuration file:

```
save config
```

Example

Enable the SSHv2 server:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags sshd
Switch:1(config)#save config
```

Changing the SSH server authentication mode

Use this procedure to change the SSH server authentication mode from the default of password-authentication to keyboard-interactive.

About this task

If you enable keyboard-interactive authentication mode, the server uses that mode over other authentication methods, except for public-key authentication, if the SSH client supports it.

If you enable keyboard-interactive authentication mode, the server generates the password prompts to display to the client rather than the client generating the prompts automatically like with password-authentication.

If you enable the ASG feature, you must change the SSH server to use keyboard-interactive authentication mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. Enable keyboard-interactive authentication:

```
ssh keyboard-interactive-auth
```

Configuring SSH configuration parameters

Configure Secure Shell version 2 (SSHv2) parameters to support public and private key encryption connections. The VSP switch does not support SSHv1.

About this task

You must enable SSH globally before you can generate SSH DSA user keys.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure the authentication type to use:

```
ssh authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256] }
```

3. Enable DSA authentication:

```
ssh dsa-auth
```

4. Generate a new DSA host key:

```
ssh dsa-host-key [<1024-1024>]
```

5. Generate a new SSHv2 DSA user key:

```
ssh dsa-user-key WORD<1-15> [size [<1024-1024>]]
```

6. Configure the type of encryption to use:

```
ssh encryption-type {[3des-cbc] [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [aes128-cbc] [aes128-ctr] [aes192-cbc] [aes192-ctr] [aes256-cbc] [aes256-ctr] [blowfish-cbc] [rijndael128-cbc] [rijndael192-cbc]}
```

7. Configure the key-exchange to use:

```
ssh key-exchange-method {[diffie-hellman-group1-sha1] [diffie-hellman-group14-sha1]}
```

8. Configure the maximum number of SSHv2 sessions:

```
ssh max-sessions <0-8>
```

9. Enable password authentication:

```
ssh pass-auth
```

10. Configure the SSHv2 connection port:

```
ssh port <22,1024..49151>
```

11. Enable RSA authentication:

```
ssh rsa-auth
```

12. Generate a new RSA host key:

```
ssh rsa-host-key [<1024-2048>]
```

13. Enable SSH secure mode:

```
ssh secure
```

14. Configure the authentication timeout:

```
ssh timeout <1-120>
```

15. Configure the SSH version:

```
ssh version <v2only>
```


Example

Enable DSA authentication and configure the maximum number of SSHv2 sessions:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ssh dsa-auth
Switch:1(config)#ssh max-sessions 5
```

Variable definitions

Use the data in the following table to use the `ssh` command.

Table 51: Variable definitions

Variable	Value
authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]}	<p>Specifies the authentication type. Select from one of the following:</p> <ul style="list-style-type: none"> • aead-aes-128-gcm-ssh • aead-aes-256-gcm-ssh • hmac-sha1 • hmac-sha2-256 <p>Use the <code>no</code> operator before this parameter, <code>no ssh authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]}</code>, to disable the authentication type. To disable all authentication types use the command <code>no ssh authentication-type</code>.</p>
dsa-auth	<p>Enables or disables the DSA authentication. The default is enabled. Use the <code>no</code> operator before this parameter, <code>no ssh dsa-auth</code>, to disable DSA authentication.</p>
dsa-host-key [<1024–1024>]	<p>Generates a new SSHv2 DSA host key. The DSA host key is 1024. Use the <code>no</code> operator before this parameter, <code>no ssh dsa-host-key</code>, to disable SSH DSA host key.</p>
dsa-user-key WORD <1–15>	<p>Generates a new SSHv2 DSA user key. WORD<1–15> specifies the user access level.</p> <p>You must enable SSH globally before you can generate SSH DSA user keys.</p> <p>If enhanced secure mode is disabled, the valid user access levels for the switch are:</p> <ul style="list-style-type: none"> • rwa — Specifies read-write-all. • rw — Specifies read-write. • ro — Specifies read-only. • rwl1 — Specifies read-write for Layer 1. • rwl2 — Specifies read-write for Layer 2.

Table continues...

Variable	Value
	<ul style="list-style-type: none"> • <code>rw13</code> — Specifies read-write for Layer 3. <p>If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role.</p> <p>If enhanced secure mode is enabled, the value user access levels for the switch are:</p> <ul style="list-style-type: none"> • <code>admin</code>—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles. • <code>operator</code>—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands. • <code>auditor</code>—Specifies a user role that can view log files and view all configurations, except password configuration. • <code>security</code>—Specifies a user role with access only to security settings and the ability to view the configurations. • <code>priv</code>—Specifies a user role with access to all of the commands that the administrator has access to, and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the VSP switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only. <p>Use the <code>no</code> operator before this parameter, <code>no ssh dsa-user-key WORD<1-15></code>, to disable SSH DSA user key.</p>
<code>encryption-type</code> {[3des-cbc] [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [aes128-cbc][aes128-ctr] [aes192-cbc][aes192-ctr] [aes256-cbc][aes256-ctr] [blowfish-cbc] [rijndael128-cbc] [rijndael192-cbc]}	<p>Configures the <code>encryption-type</code>. Select an encryption-type from one of the following:</p> <ul style="list-style-type: none"> • 3des-cbc • aead-aes-128-gcm-ssh • aead-aes-256-gcm-ssh • aes128-cbc • aes128-ctr • aes192-cbc • aes192-ctr • aes256-cbc • aes256-ctr • blowfish-cbc • rijndael128-cbc

Table continues...


Variable	Value
	<ul style="list-style-type: none"> • <code>rijndael192-cbc</code> <p>Use the <code>no</code> operator before this parameter, <code>no ssh encryption-type { [3des-cbc] [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [aes128-cbc] [aes128-ctr] [aes192-cbc] [aes192-ctr] [aes256-cbc] [aes256-ctr] [blowfish-cbc] [rijndael128-cbc] [rijndael192-cbc] }</code>, to disable the encryption type. To disable all authentication types use the command <code>no ssh encryption-type</code>.</p>
<code>key-exchange-method</code> {[diffie-hellman-group1-sha1][diffie-hellman-group14-sha1]}	<p>Configures the key-exchange type. Select from one of the following:</p> <ul style="list-style-type: none"> • <code>diffie-hellman-group1-sha1</code> • <code>diffie-hellman-group14-sha1</code> <p>Use the <code>no</code> operator before this parameter, <code>no ssh key-exchange-method { [diffie-hellman-group1-sha1] [diffie-hellman-group14-sha1] }</code>, to disable the key exchange method. To disable all authentication types use the command <code>no ssh key-exchange-method</code>.</p>
<code>max-sessions</code> <0-8>	Specifies the maximum number of SSHv2 sessions allowed. A value from 0 to 8. Default is 4.
<code>pass-auth</code>	Enables password authentication. The default is enabled.
<code>port</code> <22,1024–49151>	<p>Configures the SSHv2 connection port. <22,1024..49151> is the TCP port number. The default is 22.</p> <p> Important:</p> <p>You cannot configure the TCP port 6000 as SSH connection port.</p>
<code>rsa-auth</code>	<p>Enables RSA authentication. The default is enabled.</p> <p>Use the <code>no</code> operator before this parameter, <code>no ssh rsa-auth</code>, to disable RSA authentication.</p>
<code>rsa-host-key</code> [<1024–2048>]	<p>Generates a new SSHv2 RSA host key. Specify an optional key size of 1024 or 2048. The RSA host key can only be in a multiple of 1024. The default is 2048.</p> <p>Use the <code>no</code> operator before this parameter, <code>no ssh rsa-host-key</code>, to disable SSHv2 RSA host key.</p>
<code>rsa-user-key</code> [<1–15>]	<p>Generates a new SSHv2 RSA user key. WORD<1–15> specifies the user access level.</p> <p>You must enable SSH globally before you can generate SSH RSA user keys.</p> <p>If enhanced secure mode is disabled, the valid user access levels for the switch are:</p> <ul style="list-style-type: none"> • <code>rwa</code> — Specifies read-write-all. • <code>rw</code> — Specifies read-write. • <code>ro</code> — Specifies read-only.

Table continues...

Variable	Value
	<ul style="list-style-type: none"> • <code>rw1</code> — Specifies read-write for Layer 1. • <code>rw2</code> — Specifies read-write for Layer 2. • <code>rw3</code> — Specifies read-write for Layer 3. <p>If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role.</p> <p>If enhanced secure mode is enabled, the value user access levels for the switch are:</p> <ul style="list-style-type: none"> • <code>admin</code>—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles. • <code>operator</code>—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands. • <code>auditor</code>—Specifies a user role that can view log files and view all configurations, except password configuration. • <code>security</code>—Specifies a user role with access only to security settings and the ability to view the configurations. • <code>priv</code>—Specifies a user role with access to all of the commands that the administrator has access to, and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the VSP switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only. <p>Use the <code>no operator</code> before this parameter, <code>no ssh rsa-user-key WORD<1-15></code>, to disable SSH RSA user key.</p>
<code>secure</code>	<p>Enables SSHv2 in secure mode and immediately disables the access services SNMP, FTP, TFTP, rlogin, and Telnet. The default is disabled.</p> <p>Use the <code>no operator</code> before this parameter, <code>no ssh secure</code>, to disable SSHv2 in secure mode.</p>
<code>timeout <1-120></code>	<p>Specifies the SSHv2 connection authentication timeout in seconds. Default is 60 seconds.</p>
<code>version <v2only></code>	<p>Configures the SSH version. The default is <code>v2only</code>.</p> <p>The switch only supports SSHv2.</p>

Verifying and displaying SSH configuration information

Verify that SSHv2 services are enabled on the VSP switch and display SSHv2 configuration information to ensure that the SSHv2 parameters are properly configured.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Verify that SSHv2 services are enabled and view the SSHv2 configuration:

```
show ssh <global|session>
```

Example

Display global system SSHv2 information:

```
Switch:1(config)#show ssh global
Total Active Sessions      : 0
  version                  : v2only
  port                     : 22
  max-sessions             : 4
  timeout                  : 60
  action rsa-host key     : rsa-hostkeysize 2048
  action dsa-host key     : dsa-hostkeysize 1024
  rsa-auth                 : false
  dsa-auth                 : true
  pass-auth                : true
  keyboard-interactive-auth : false
  sftp enable              : true
  enable                   : true
  authentication-type     : aead-aes-128-gcm-ssh aead-aes-256-gcm-ssh hmac-sha1
hmac-sha2-256
  encryption-type         : 3des-cbc aead-aes-128-gcm-ssh aead-aes-256-gcm-ssh
aes128-cbc aes128-ctr
                           aes192-cbc aes192-ctr aes256-cbc aes256-ctr blowfish-
cbc rijndael128-cbc
                           rijndael192-cbc
  key-exchange-method     : diffie-hellman-group1-sha1 diffie-hellman-group14-sha1
```

Variable definitions

Use the data in the following table to use the `show ssh` command.

Table 52: Variable definitions

Variable	Value
global	Display global system SSH information.
session	Display the current session SSH information.

Connecting to a remote host using the SSH client

Configure the SSHv2 parameters to connect to a remote host.

Before you begin

- You must enable the SSHv2 server.

About this task

The command format, for the ACLI SSH client command, is similar to Telnet with two additional parameters: `-l` login and an optional `-p` port parameter.

Procedure

- Enter the Privileged EXEC mode:

```
enable
```

- Connect to a remote host:

```
ssh WORD<1-256> -l WORD<1-32> [-p <1-32768>]
```

Example

Connect to the remote host:

```
Switch:1>enable
Switch:1#ssh 192.0.2.1 -l rwa
```

Variable definitions

Use the following table to use the `ssh` command.

Table 53: Variable definitions

Variable	Value
WORD<1-32>	Specifies the user login name of the remote SSH server.
-p <1-32768>	Specifies the port number to connect to the remote SSH server. The default is 22.

Generating user key files

Configure the SSHv2 parameters to generate DSA user key files.

Before you begin

- You must enable the SSHv2 server.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create the DSA user key file:

```
ssh dsa-user-key [WORD<1-15>][size <1024-1024>]
```

3. Enter the encryption password to protect the key file.
4. Copy the user public key file to the remote SSH servers.
5. If you are generating the compatible keys on the Linux system, use the following steps:

- a. Create the DSA user key file:

```
ssh-keygen -t dsa
```

- b. Copy the user public key to the remote SSH servers.

*** Note:**

The DSA pair key files can be generated on the Linux system and used by the VSP switch SSH client.

Example

Create the DSA user key file with the user access level set to read-write-all and size of the DSA user key set to 512 bits:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ssh dsa-user-key rwa size 512
```

Variable definitions

Use the following table to use the `ssh dsa-user-key` command.

Table 54: Variable definitions

Variable	Value
<code>WORD<1-15 ></code>	<p>Generates a new SSHv2 DSA user key. <code>WORD<1-15></code> specifies the user access level.</p> <p>If enhanced secure mode is disabled, the valid user access levels for the switch are:</p> <ul style="list-style-type: none"> • <code>rwa</code> — Specifies read-write-all. • <code>rw</code> — Specifies read-write. • <code>ro</code> — Specifies read-only. • <code>rw1</code> — Specifies read-write for Layer 1.

Table continues...

Variable	Value
	<ul style="list-style-type: none"> • <code>rw12</code> — Specifies read-write for Layer 2. • <code>rw13</code> — Specifies read-write for Layer 3. <p>If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role.</p> <p>If enhanced secure mode is enabled, the value user access levels for the switch are:</p> <ul style="list-style-type: none"> • <code>admin</code>—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles. • <code>operator</code>—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands. • <code>auditor</code>—Specifies a user role that can view log files and view all configurations, except password configuration. • <code>security</code>—Specifies a user role with access only to security settings and the ability to view the configurations. • <code>priv</code>—Specifies a user role with access to all of the commands that the administrator has access to, and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the VSP switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only. <p>Use the <code>no operator</code> before this parameter, <code>no ssh dsa-user-key WORD<1-15></code>, to disable SSH DSA user key.</p>
size <1024-1024>	Specifies the size of the DSA user key. The default is 1024 bits.

Managing an SSL certificate

The TLS server selects the server certificate in the following order:

1. A CA-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.
2. A self-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.

If the server certificates are not available, TLS server generates a new self-signed certificate on boot and uses that by default. The self-signed certificate is available in `/.intflash/.cert/.ssl`. You can choose to use an online or offline CA signed certificate which will take precedence over the self-signed one.

About this task

If a certificate is already present, you must confirm that it can be deleted before a new one is created.

After you create a certificate, the system logs one of the following INFO alarms:

- New default Server Certificate and Key are generated and installed
- Current Server Certificate and Key are installed

The default certificate key length for a certificate generated on the switch is 2,048 bits.

* Note:

The `ssl certificate [validity-period-in-days <30-3650>]` command in this procedure does not require a system reboot.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create and install a new self-signed certificate:

```
ssl certificate [validity-period-in-days <30-3650>]
```

3. Delete a certificate:

```
no ssl certificate
```

* Note:

The certificate loaded in memory remains valid until you use the `ssl reset` command or reboot the system.

Variable definitions

Use the data in the following table to use the `ssl certificate` command.

Variable	Value
validity-period-in-days <30-3650>	Specifies an expiration time for the certificate. The default is 365 days.

Disabling SFTP without disabling SSH

Disable SFTP while allowing SSH to remain active.

Before you begin

Enhanced secure mode must be enabled. For information about enabling enhanced secure mode, see [Enabling enhanced secure mode](#) on page 225.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable the SSHv2 server:

```
enable ssh sftp
```

3. Save the configuration file:

```
save config
```

Enabling SSH rekey

Before you begin

Enable SSH globally.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
ssh rekey enable
```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Enable SSH rekeying globally:

```
Switch:1(config)#ssh rekey enable
```

Variable Definitions

Use the data in the following table to use the `ssh rekey` command.

Variable	Value
enable	Enables SSH rekey globally.

Configuring SSH rekey data-limit

Use the following procedure to configure the limit for data transmission during the session.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
ssh rekey data-limit <1-6>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Configure the SSH rekey data-limit to 2 GB:

```
Switch:1(config)#ssh rekey data-limit 2
```

Variable definitions

Use the following table to use the `ssh rekey data-limit` command.

Variable	Value
<1-6>	Sets the SSH rekey data limit in GB, range is 1-6.

Configuring SSH rekey time-interval

Use the following procedure to configure a time interval, after which the key exchange takes place.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Enter the following command:


```
ssh rekey time-interval <1-6>
```

Example

```
Switch:1> enable
Switch:1# configure terminal
```

Configure the SSH rekey time-interval to 3 hours:

```
Switch:1(config)# ssh rekey time-interval 3
```

Variable definitions

Use the data in the following table to use the `ssh rekey time-interval` command.

Variable	Value
<1-6>	Sets the time-interval for SSH rekeying in hours, the range is 1 to 6.

Displaying SSH rekey information

Use the following procedure to display the SSH rekey information.

Procedure

1. Enter Privileged EXEC mode:


```
enable
```
2. Enter the following command:


```
show ssh rekey
```

Example

```
Switch:1> enable
Switch:1#show ssh rekey
  Rekey Status      : TRUE
```

```
Rekey data limit      : 1 GB
Rekey time interval  : 1 hours
```

Field descriptions

The following table describes the output for the `show ssh rekey` command.

Name	Description
Rekey status	Displays the status (TRUE or FALSE) of SSH rekeying.
Rekey data limit	Displays the configured SSH rekey data transmission limit GB.
Rekey time interval	Displays the configured SSH rekey time interval in hours.

Downgrading or upgrading from releases that support different key sizes

Use this procedure if you need to downgrade or upgrade from a release that supports different key sizes.

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the `.ssh` directory and generate new keys for SSH. If you do not do this, key sizes that are no longer supported will no longer function.

For more information about supported software, see *Release Notes for VSP Operating System Software*, NN47227-401.

You only need to perform this procedure if you have previously generated DSA host, RSA host, or DSA user keys with a release that supports different key sizes.

Procedure

1. Use the following command to disable SSH:

```
no ssh
```

2. From the config terminal go to the `.ssh` directory using the command:

```
cd /intflash/.ssh
```

3. After you upgrade or downgrade, delete the following keys from the `.ssh` directory.

```
ssh_dss.key
ssh_rsa.key
moc_sshc_dsa_file
moc_sshc_rsa_file
id_dsa_rwa
```

Secure Shell configuration using ACLI

```
id_dsa_rwa.pub
id_rsa_rwa
id_rsa_rwa.pub
moc_sshc_dsa_file_fed
moc_sshc_rsa_file_fed
known_hosts
ssh_ecdsa.key
dsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
example: dsa_key_rwa
rsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
example: rsa_key_rwa
```

4. Generate a new DSA host key:

```
ssh dsa-host-key [<1024-1024>]
```

5. Generate a new SSH DSA user key:

```
ssh dsa-user-key WORD<1-15> [size <1024-1024>]
```

6. Generate a new RSA host key:

```
ssh rsa-host-key [<1024-2048>]
```

Chapter 26: Secure Shell configuration using Enterprise Device Manager

Use Secure Shell version 2 (SSHv2) to enable secure communications support over a network for authentication, encryption, and network Integrity.

VSP 4000 supports both SSHv2 server and SSHv2 client.

For more information, see [Changing Secure Shell configuration parameters](#) on page 202.

For information about downloading and enabling security encryption, see [Downloading the software](#) on page 201.

Downloading software from the Avaya support site

Download new software to upgrade the Avaya Virtual Services Platform 4000 Series. Software downloads can include encryption modules and software images.

Before you begin

- You must have access to the new software from the Avaya support site: <https://support.avaya.com>. You need a valid user or site ID and password.

About this task

Download the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) software before you enable the encryption algorithms and use SNMPv3. The AES and DES encryption modules exist in a single file.

Caution:

To download the software and files, use one of the following browsers: IE 9 or greater, or Mozilla Firefox.

Download the SSH encryption software before you enable the 3DES encryption module and use SSH.

Due to export restrictions, the encryption capability is separate from the main software image. SNMPv3 and the SSH server do not function properly without the use of this image.

For more information about file names for the current release, see *Release Notes for VSP Operating System Software*, NN47227-401.

Procedure

1. From an Internet browser, browse to <https://support.avaya.com>.
2. Under **Support by Product**, select **Downloads**.
3. In the product search field, type **Virtual Services Platform 4000**.
4. In the **Choose Release** field, click a release number.
5. Click the download title to view the selected information.
6. Click the file you want to download.
7. Login to download the required software file.
8. Use an FTP client in binary mode to transfer the file to the Virtual Services Platform 4000.

Changing Secure Shell parameters

You can use Enterprise Device Manager to change the SSHv2 configuration parameters. However, Avaya recommends using the ACLI to perform the initial configuration of SSHv2. The VSP switch does not support SSHv1.

Before you begin

The user access level is read/write/all community strings.

To enable SSH, ensure to enable rsa-auth or dsa-auth, or both.

About this task

If the SSH service is enabled, all fields are dimmed until the SSHv2 service is disabled. You must disable the SSHv2 service before setting the SSHv2 service parameters.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **SSH**.
3. In the **Enable** options, choose the type of SSH service you want to enable.
4. In the **Version** options, choose a version.
5. In the **Port** field, type a port.
6. In the **MaxSession** field, type the maximum number of sessions allowed.
7. In the **Timeout** field, type the timeout.
8. From the **KeyAction** options, choose a key action.
9. In the **RsaKeySize** box, type the RSA key size.

10. In the **DSAKeySize** field, type the DSA key size.
11. Select the **RsaAuth** box for RSA authentication if desired.
12. Select the **DsaAuth** box for DSA authentication if desired.
13. Select the **PassAuth** box for password authentication if desired.
14. Select the **SftpEnable** box if you want SFTP enabled.
15. Select the **KeyboardInteractiveAuth** if you want keyboard interactive authentication enabled.
16. In the **AuthType** section, select the authentication types you want.
17. In the **EncryptionType** section, select the encryption types you want.
18. In the **KeyExchangeMethod** section, select the key exchange methods you want.
19. Click **Apply**.

SSH field descriptions

Use the data in the following table to use the **SSH** tab.



Name	Description
Enable	<p>Enables, disables, or securely enables SSHv2. The options are:</p> <ul style="list-style-type: none"> • false • true • secure <p>Select false to disable SSHv2 services. Select true to enable SSHv2 services. Select secure to enable SSHv2 and disable access services (SNMP, FTP, TFTP, rlogin, and Telnet). The default is false.</p> <p> Important:</p> <p>Do not enable SSH secure mode using Enterprise Device Manager. Enabling secure mode disables SNMP. This locks you out of the Enterprise Device Manager session. Enable SSH secure mode using ACLI.</p>
Version	<p>Configures the SSH version. The options are:</p> <ul style="list-style-type: none"> • v2only <p>The default is v2only.</p>
Port	<p>Configures the SSHv2 connection port number. <22 or 1024–49151> is the port range of SSH.</p> <p> Important:</p> <p>You cannot configure the TCP port 6000 as SSHv2 connection port.</p>
MaxSession	Configures the maximum number of SSHv2 sessions allowed.

Table continues...

Name	Description
	The value can be from 0 to 8. The default is 4.
Timeout	Configures the SSHv2 authentication connection timeout in seconds. The default is 60 seconds.
KeyAction	Configures the SSHv2 key action. The options are: <ul style="list-style-type: none"> • none • generateDsa • generateRsa • deleteDsa • deleteRsa
RsaKeySize	Configures SSHv2 RSA key size. The value can be from 1024 or 2048. The RSA key size can only be a multiple of 1024. The default is 2048.
DsaKeySize	Configures the SSHv2 DSA key size. By default, 1024 is the only key size.
RsaAuth	Enables or disables SSHv2 RSA authentication. The default is enabled.
DsaAuth	Enables or disables SSHv2 DSA authentication. The default is enabled.
PassAuth	Enables or disables SSHv2 RSA password authentication. The default is enabled.
SftpEnable	Enables or disables SFTP.
KeyboardInteractiveAuth	Enables or disables keyboard interactive authentication.
AuthType	Specifies the authentication type. Select from one of the following: <ul style="list-style-type: none"> • hmacSha1 • hmac-sha2-256 • aeadAes128GcmSsh • aeadAes-256GcmSsh
EncryptionType	Configures the encryption-type. Select an encryption-type from one of the following: <ul style="list-style-type: none"> • aes128Cbc • aes256Cbc • threeDesCbc • aeadAes128GcmSsh • aeadAes256GcmSsh • aes128Ctr • rijndael128Cbc • aes256Ctr • aes192Ctr • aes192Cbc

Table continues...

Name	Description
	<ul style="list-style-type: none">• aes256-ctr• rijndael192Cbc• blowfishCbc
KeyExchangeMethod	Configures the key-exchange type. Select from one of the following: <ul style="list-style-type: none">• diffieHellmanGroup14Sha1• diffieHellmanGroup1Sha1

Chapter 27: System access fundamentals

This section contains conceptual information about how to access Avaya Virtual Services Platform 4000 Series and create users and user passwords for access.

Logging on to the system

After the startup sequence is complete, the login prompt appears.

*** Note:**

With enhanced secure mode enabled, the person in the role-based authentication level of administrator configures the login and password values for the other role-based authentication levels. The administrator initially logs on to the switch using the default login of `admin` and the default password of `admin`. After the initial login, the switch prompts the administrator to create a new password.

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user. For more information on enhanced secure mode, see [System access security enhancements](#) on page 224.

The following table shows the default values for login and password for the console and Telnet sessions.

Table 55: Access levels and default logon values

Access level	Description	Default logon	Default password
Read-only	Permits view only configuration and status information. This access level is equivalent to Simple Network Management Protocol (SNMP) read-only community access.	ro	ro
Layer 1 read-write	View most switch configuration and status information and change physical port settings.	l1	l1
Layer 2 read-write	View and change configuration and status information for Layer 2 (bridging and switching) functions.	l2	l2

Table continues...

Access level	Description	Default logon	Default password
Layer 3 read-write	View and change configuration and status information for Layer 2 and Layer 3 (routing) functions.	l3	l3
Read-write	View and change configuration and status information across the switch. Read-write access does not allow you to change security and password settings. This access level is equivalent to SNMP read-write community access.	rw	rw
Read-write-all	Permits all the rights of read-write access and the ability to change security settings. This access level allows you to change the Avaya command line interface (ACLI) and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

You can enable or disable users with particular access levels, eliminating the need to maintain large numbers of access levels and passwords for each user.

The system denies access to a user with a disabled access level who attempts to log on. The following error message appears after a user attempts to log on with a blocked access level:

```
CPU1 [mm/dd/yy hh:mm:ss] 0x0019bfff GlobalRouter ACLI WARNING Slot 1: Blocked
unauthorized acli access
```

The system logs the following message to the log file:

```
User <user-name> tried to connect with blocked access level <access-level> from <src-
ipaddress> via <login type>.
```

The system logs the following message for the console port:

```
User <user-name> tried to connect with blocked access level <access-level> from console
port.
```

RADIUS authentication

Remote Authentication Dial-in User Service (RADIUS) authentication takes precedence over the local configuration. If you enable RADIUS authentication on the switch, the user can access the switch even if you block an access level on the switch.

Important:

When you enable RADIUS on the switch and configure a RADIUS server to be used by CLI or EDM, the server authenticates the connection, whether it is FTP, HTTPS, SSH, or TELNET. However, in the event that the RADIUS server is unresponsive or is unreachable, the switch will fall back to the local authentication, so that you can access the switch using your local login credentials.

If you disable an access level, all running sessions, except FTP sessions, with that access level to the switch terminate.

! Important:

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

The system preserves these configurations across restarts.

hsecure bootconfig flag

Virtual Services Platform 4000 supports a configurable flag called high secure (hsecure). Use the hsecure flag to enable the following password features:

- 10 character enforcement
- Aging time
- Limitation of failed login attempts
- Protection mechanism to filter designated IP addresses

If you activate the `hsecure` flag, the software enforces the 10-character rule for all passwords. The password must contain a minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

If you enable hsecure for the first time and the password file does not exist, then the device creates a normal default username (rwa) and password (rwa). In this case, the password does not meet the minimum requirements for hsecure and as a result the system prompts you to change the password.

For more information about the hsecure flag, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601.

Enhanced secure mode

If you enable enhanced secure mode, the system has new authentication levels. Enhanced secure mode allows the system to:

- Provide role-based access levels
- Stronger password requirements
- Stronger rules on password length
- Stronger rules on password complexity
- Stronger rules on password change intervals
- Stronger rules on password reuse
- Stronger password maximum age use

For more information on enhanced secure mode, see [System access security enhancements](#) on page 224.

Managing the system using different VRF contexts

You can use the Enterprise Device Manager (EDM) to manage the system using different Virtual Router Forwarding (VRF) contexts.

- Using the GlobalRouter (VRF 0), you can manage the entire system. GlobalRouter is the default view at log in
- Using a VRF context other than the GlobalRouter (VRF 0), you have limited functionality to manage the system. For instance you can only manage the ports assigned to the specified VRF instance

Specify the VRF instance name on the EDM screen when you launch a VRF context view. You can use the context names (SNMPv3) and community strings (SNMPv1/v2) to assign different VRFs to manage selected components, such as ports and VLANs. For more information about context names and community strings, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

ACL I passwords

The switch ships with default passwords set for access to ACL I through a console or Telnet session. If you possess read-write-all access authority, and you use SNMPv3, then you can change passwords in encrypted format. If you use Enterprise Device Manager (EDM), then you can also specify the number of allowed Telnet sessions and rlogin sessions.

Important:

Be aware that the default passwords and community strings are documented and well known. Avaya strongly recommends that you change the default passwords and community strings immediately after the first logon.

For security, if you fail to log on correctly on the device in three consecutive instances, then the device locks for 60 seconds.

Virtual Services Platform 4000 stores passwords in encrypted format and not in the configuration file.

Subscriber or administrative interaction

As a network administrator, you can configure the RADIUS server for user authentication to override user access to commands. You must still provide access based on the existing access levels in Virtual Services Platform 4000, but you can customize user access by allowing and denying specific commands.

You must configure the following three returnable attributes for each user:

- Access priority (single instance)—the access levels currently available on Virtual Services Platform 4000 (ro, l1, l2, l3, rw, rwa)
- Command access (single instance)—indicates whether the user has access to the commands on the RADIUS server
- ACL I commands (multiple instances)—the list of commands that the user can or cannot use

Access policies for services

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), Secure Shell version 2 (SSHv2), and remote login (rlogin). You can enable or disable access services by configuring flags.

Avaya recommends that you use access policies for in-band management to secure access to the switch. By default, all services are denied. You must enable the default policy or enable a custom policy to provide access. A lower precedence takes higher priority if you use multiple policies. Preference 120 has priority over preference 128.

You can define network stations that can access the switch or stations that cannot access the switch. For each service you can also specify the level of access, such as read-only or read-write-all.

When you configure access policies, you can perform either of the following actions:

- Globally enable the access policy feature, and then create and enable individual policies. Each policy takes effect immediately after you enable it.
- Create and enable individual access policies, and then globally enable the access policy feature to activate all the policies at the same time.

HTTP, SSH and rlogin support IPv4.

Web interface passwords

Virtual Services Platform 4000 includes a Web-management interface, Enterprise Device Manager (EDM), that you can use to monitor and manage the device through a supported Web browser from anywhere on the network. For more information on supported web browsers, see *Using CLI and EDM on VSP Operating System Software*, NN47227-103.

A security mechanism protects EDM and requires you to log on to the device using a user name and password. The default user name is `admin` and the default password is `password`.

Important:

For security reasons, EDM is disabled by default. For instructions about how to enable the interface, see *Quick Start for Avaya Virtual Services Platform 4000 Series*, NN46251-102.

Password encryption

Virtual Services Platform 4000 handles password encryption in the following manner:

- After the device starts, the system restores the web-server passwords and community strings from the hidden file.
- After you modify the web-server username and password or SNMP community strings, the system makes the modifications to the hidden file.

Enhanced secure mode authentication access levels

After you enable enhanced secure mode with the `boot config flags enhancedsecure-mode` command, the switch supports role-based authentication levels. With enhanced secure mode enabled, the switch supports the following authentication access levels for local authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

Each username is associated with a certain role in the product and appropriate authorization rights for viewing and executing commands are available for that role.

With enhanced secure mode enabled, the person in the role-based authentication level of administrator configures the login and password values for the other role-based authentication levels.

The administrator initially logs on to the switch using the default login of `admin` and the default password of `admin`. After the initial login, the switch prompts the administrator to create a new password.

The following displays an example of the initial login to the switch by the administrator after enhanced secure mode is enabled.

```

Login: admin
Password: *****
      This is an initial attempt using the default user name and password.
      Please change the user name and password to continue.
Enter the new name : rwa
Enter the New password : *****
Re-enter the New password : *****
Password changed successfully
      Last Successful Login:Wed Oct 14 12:20:42 2015
      Unsuccessful Login attempts from last login is: 0

```

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user.

Access level and login details

Access level	Description	Login location
Administrator	The administrator access level permits all read-write access, and can change security settings. The administrator access level can configure ACLI and web-based management user names,	SSH/Telnet (in band/mgmt)/ console

Table continues...

Access level	Description	Login location
	passwords, and the SNMP community strings. The administrator access level can also view audit logs.	
Privilege	The privilege access level has the same access permission as the administrator; however, the privilege access level cannot use RADIUS or TACACS+ authentication. The system must authenticate the privilege access level within the switch at a console level. The privilege access level is also known as emergency-admin.	console
Operator	The operator access level can view most switch configurations and status information. The operator access level can change physical port settings at layer 2 and layer 3. The operator access level cannot access audit logs or security settings.	SSH/Telnet(in band/mgmt)/ console/
Auditor	The auditor access level can view configuration information, status information, and audit logs.	SSH/Telnet(in band/mgmt)/ console/
Security	The security access level can change security settings only. The security access level also has permission to view configuration and status information.	SSH/Telnet(in band/mgmt)/ console/

Password requirements

After you enable enhanced secure mode on the switch the password requirements are stronger. The individual in the administrator access level role configures and provides a temporary user name and password. After you log in for the first time with the temporary user name and temporary password, the system forces you to change the temporary password. After you change the temporary password, you cannot use the password again in subsequent sessions.

The following topic discusses the enhanced password requirements.

Password complexity rule

After you enable enhanced secure mode, the system checks each password change request to ensure the new password meets the password complexity required.

The default for the password complexity rule includes the following:

- Two uppercase character, from the range: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Two lowercase character, from the range: abcdefghijklmnopqrstuvwxyz
- Two numeric character, from the range: 1234567890
- Two special character, from the range: `~!@#\$%^&*()_+={}|~\|:;'"<>./?

Password length rule

The system enforces a minimum password length of 15 characters after you enable enhanced secure mode.

If you do not meet the password length rule, the system displays the following message:

```
Password change aborted. The new password does not meet the minimum complexity requirement. Please select another password that meets the change interval, length, complexity, no consecutive repeating characters or history requirements of the domain.
```

Password change interval rule

The system enforces a minimum password change interval, which defines the minimum amount of time before you can change to a new password. By default, the minimum change interval is 24 hours between changing from one password to a new password. If you want to change your password, and attempt to do so, the system checks the timestamp for your password to determine if enough time has passed to allow you to change the password.

If you attempt to change the password and not enough time has passed, the system rejects the request, and the system informs you that the password was recently changed. Any password change outside of the enforced interval requires the Administrator to approve the change.

If you try to change the password before the change interval allows, the system displays the following message:

```
Password change aborted. The new password does not meet the minimum complexity requirement. Please select another password that meets the change interval, length, complexity, no consecutive repeating characters or history requirements of the domain.
```

Password reuse rule

After you enable enhanced secure mode, the administrator access level can define the number of old passwords that cannot be reused. The password reuse rule ensures that recently used passwords are not reused immediately, which reduces the risk of someone unlawfully gaining access to the system. The default number of prohibited recently used passwords is 3, but you can define up to 99.

The system saves the password history and stores the history in an encrypted format, along with the user name, and date of change. If a particular user attempts to change a password, the system looks up the password history list, and checks it against the stored passwords the user has previously used. If the password is on the list of previously used passwords, the system rejects the password change, and displays the following message:

```
Old password not allowed.
```

Password maximum age rule

The system enforces automatic password renewal and password lockout after the expiration period because long-term usage of the same password can cause the system to be vulnerable to hacking.

You can configure the password expiration period to a range of 1 to 365 days. The default password expiration period is 90 days.

Password max-session

The password max-sessions value indicates the maximum number of times a particular type of role-based user can log in to the switch through the SSH session at the same time. The max-sessions value applies only for SSH sessions, and only with enhanced secure mode enabled.

After the maximum session number is reached that particular type of user cannot login. For example, if the max-sessions for an auditor user is configured as 5, then the auditor user can log in to only five SSH sessions at the same time. The default is 3.

Password pre-notification interval and post-notification interval rule

After enhanced secure mode is enabled, the switch enforces password expiry. To ensure a user does not lose access, the switch offers pre- and post-notification messages explaining when the password will expire.

The administrator can define pre- and post-notification intervals to between one to 99 days.

The system maintains the password with a time stamp for when the password expiration. When you log in, the system checks the password time stamp and the notification timer values. If the administrator configures the pre-notification to 30 days, when you log in, the system checks the time stamp and notification timer values, and if the password expiry is due in 30 days, the system displays the first notification.

The pre-notification intervals provide messages to warn users that their passwords will expire within a particular timeframe:

- interval 1—By default, interval 1 is 30 days.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 1 day.

The post-notification intervals provide notification to users that their passwords have expired within a particular timeframe:

- interval 1—By default, interval 1 is 1 day.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 30 days.

If you do not change the password before the expiry date, the system locks your account. Once locked, only the administrator can unlock the account. The administrator creates a temporary password, and then you can login with the temporary password.

Chapter 28: System access configuration using ACLI

The section provides procedures to manage system access through configurations such as usernames, passwords, and access policies.

Enabling ACLI access levels

About this task

Enable ACLI access levels to control the configuration actions of various users.

Important:

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

The system preserves these configurations across restarts.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable an access level:

```
password access-level WORD<2-8>
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
```

Block ACLI access to Layer 1 to control the configuration actions of various users:

```
VSP-4850GTS-PWR+:1(config)#no password access-level 11
```

Variable definitions

Use the data in the following table to use the `password access-level` command.

Table 56: Variable definitions

Variable	Value
<code>WORD<2-8></code>	<p>Permits or blocks this access level. The available access level values are as follows:</p> <ul style="list-style-type: none"> • l1 — Specifies Layer 1. • l2 — Specifies Layer 2. • l3 — Specifies Layer 3. • ro — Specifies read-only. • rw — Specifies read-write. • rwa — Specifies read-write-all. <p>To set this option to the default value, use the default operator with the command. By default, the system permits all access levels. To block an access level, use the no operator with the command.</p>

Changing passwords

Before you begin

- You must use an account with read-write-all privileges to change passwords. For security, the switch saves passwords to a hidden file.

About this task

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive Avaya Virtual Services Platform 4000 Series, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

If you enable the `hsecure` flag, after the aging time expires, the system prompts you to change your password. If you do not configure the aging time, the default is 90 days.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Change a password:

```
cli password WORD<1-20> {layer1|layer2|layer3|read-only|read-write|
read-write-all}
```

3. Enter the old password.
4. Enter the new password.
5. Enter the new password a second time.
6. Configure password options:

```
password [access-level WORD<2-8>] [aging-time <1-365>] [default-
lockout-time <60-65000>] [lockout WORD<0-46> time <60-65000>] [min-
passwd-len <10-20>] [password-history <3-32>]
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Change a password:

```
VSP-4850GTS-PWR+:1(config)#cli password smith read-write-all
```

Enter the old password:

```
VSP-4850GTS-PWR+:1(config)#winter
```

Enter the new password:

```
VSP-4850GTS-PWR+:1(config)#summer
```

Enter the new password a second time:

```
VSP-4850GTS-PWR+:1(config)#summer
```

Set password to an access level of read-write-all and the expiration period for the password to 60 days:

```
VSP-4850GTS-PWR+:1(config)#password access-level rwa aging-time 60
```

Variable definitions

Use the data in the following table to use the `cli password` command.

Table 57: Variable definitions

Variable	Value
layer1 layer2 layer3 read-only read-write read-write-all	Changes the password for the specific access level.
WORD<1-20>	Specifies the user logon name.

Use the data in the following table to use the `password` command.

Table 58: Variable definitions

Variable	Value
access level WORD<2–8>	Permits or blocks this access level. The available access level values are as follows: <ul style="list-style-type: none"> • l1 • l2 • l3 • ro • rw • rwa
aging-time <1-365>	Configures the expiration period for passwords in days, from 1–365. The default is 90 days.
default-lockout-time <60-65000>	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60–65000 range. The default is 60 seconds. To configure this option to the default value, use the default operator with the command.
lockout WORD<0–46> time <60-65000>	Configures the host lockout time. <ul style="list-style-type: none"> • WORD<0–46> is the host IP address in the format a.b.c.d. • <60-65000> is the lockout-out time, in seconds, in the 60–65000 range. The default is 60 seconds.
min-passwd-len <10-20>	Configures the minimum length for passwords in high-secure mode. The default is 10 characters. To configure this option to the default value, use the default operator with the command.
password-history <3-32>	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default is 3. To configure this option to the default value, use the default operator with the command.

Configuring an access policy

About this task

Configure an access policy to control access to the switch.

You can permit network stations to access the switch or forbid network stations to access the switch.

For each service, you can also specify the level of access; for example, read-only or read-write-all.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create an access policy by assigning it a number:

```
access-policy <1-65535>
```

3. Restrict the access to a specific level:

```
access-policy <1-65535> access-strict
```

4. Configure access for an access policy:

```
access-policy <1-65535> accesslevel <ro|rwa|rw>
```

5. Configure the access policy mode, network, and precedence:

```
access-policy <1-65535> [mode <allow|deny>] [precedence <1-128>]
[network <A.B.C.D> <A.B.C.D>]
```

If you configure the access policy mode to **deny**, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to **deny**, the system does not check **accesslevel** or **access-strict** information. If you configure the access policy mode to allow, the system continues to check the **accesslevel** and **access-strict** information.

6. Configure optional access protocols for an access policy:

```
access-policy <1-65535> [ftp] [http] [ssh] [telnet] [tftp]
```

7. Configure optional trusted username access for an access policy:

```
access-policy <1-65535> host WORD<0-46> [username WORD<0-30>]
```

8. Configure optional SNMP parameters for an access policy:

```
access-policy <1-65535> [snmp-group WORD<1-32> <snmpv1|snmpv2c|usm>]
```

OR

```
access-policy <1-65535> [snmpv3]
```

9. Enable the access policy:

```
access-policy <1-65535> enable
```

10. Enable access policies globally:

```
access-policy
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Assuming no access policies exist, start with policy 3 and name the policy policy3:

```
VSP-4850GTS-PWR+:1(config)# access-policy 3 name policy3
```

Add read-write-all access level to policy 3:

```
VSP-4850GTS-PWR+:1(config)# access-policy 3 accesslevel rwa
```

Add the usm group group_example to policy 3:

```
VSP-4850GTS-PWR+:1# access-policy 3 snmp-group group_example usm
```

Enable access strict:

```
VSP-4850GTS-PWR+:1config)# access-policy 3 access-strict
```

Enable policy 3:

```
VSP-4850GTS-PWR+:1(config)# access-policy 3 enable
```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Table 59: Variable definitions

Variable	Value
access-strict	Restrains access to criteria specified in the access policy. <ul style="list-style-type: none"> • true—The system accepts only the currently configured access level. • false—The system accepts access up to the configured level. Use the no operator to remove this configuration.
accesslevel <ro rwa rw>	Specifies the level of access if you configure the policy to allow access.
enable	Enables the access policy.
ftp	Activates or disables FTP for the specified policy. Because FTP derives its login and password from the ACLI management filters, FTP works for read-write-all (rwa) and read-write (rw) access, but not for the read-only (ro) access. Use the no operator to remove this configuration.

Table continues...

Variable	Value
host <i>WORD</i> <0–46>	<p>For remote login access, specifies the trusted host address as an IP address.</p> <p>The Virtual Services Platform 9000 supports access-policies over IPv4 and IPv6 with no difference to functionality or configuration.</p> <p>Use the no operator to remove this configuration.</p>
http	<p>Activates the HTTP for this access policy. Use the no operator to remove this configuration.</p>
mode < <i>allow</i> <i>deny</i> >	<p>Specifies whether the designated network address is allowed access to the system through the specified access service. The default is allow.</p> <p>If you configure the access policy mode to deny, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to deny, the system does not check accesslevel1 or access-strict information. If you configure the access policy mode to allow, the system continues to check the accesslevel1 and access-strict information.</p>
network <A.B.C.D> <A.B.C.D>	<p>Specifies the IP address and subnet mask for IPv4 or the IP address and prefix for IPv6 that can access the system through the specified access service.</p> <p>Virtual Services Platform 9000 supports access-policies over IPv4 and IPv6 with no difference to functionality or configuration.</p> <p>Use the no operator to remove this configuration.</p>
precedence <1–128>	<p>Specifies a precedence value for a policy, expressed as a number from 1–128. The precedence value determines which policy the system uses if multiple policies apply. Lower numbers take higher precedence. The default value is 10.</p>
snmp-group <i>WORD</i> <1–32> <snmpv1 snmpv2c usm>	<p>Adds an SNMP version 3 group under the access policy.</p> <p><i>WORD</i><1–32> is the SNMP version 3 group name consisting of 1–32 characters.</p> <p><snmpv1 snmpv2c usm> is the security model; either snmpv1, snmpv2c, or usm.</p> <p>Use the no operator to remove this configuration.</p>
snmpv3	<p>Activates SNMP version 3 for the access policy.</p> <p>Use the no operator to remove this configuration.</p>
ssh	<p>Activates SSH for the access policy.</p>

Table continues...

Variable	Value
	Use the no operator to remove this configuration.
telnet	Activates Telnet for the access policy. Use the no operator to remove this configuration.
tftp	Activates the Trivial File Transfer Protocol (TFTP) for this access policy. Use the no operator to remove this configuration.
username <i>WORD</i> <0–30>	Specifies the trusted host user name for remote login access.

Specifying a name for an access policy

About this task

Assign a name to an existing access policy to uniquely identify the policy.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Assign a name to the access policy:

```
access-policy <1-65535> name WORD<0-15>
```

Example

```
VSP-4850GTS-PWR+:1>enable
VSP-4850GTS-PWR+:1#configure terminal
```

Assign a name to an access policy:

```
VSP-4850GTS-PWR+:1(config)#access-policy 10 name useraccounts
```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Table 60: Variable definitions

Variable	Value
name <i>WORD</i> <0–15>	Specifies a name expressed as a string from 0–15 characters.

Allowing a network access to the switch

About this task

Specify the network to which you want to allow access.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Specify the network:

```
access-policy <1-65535> [mode <allow|deny>] [network <A.B.C.D>
<A.B.C.D>]
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

Specify the network to which you want to allow access:

```
VSP-4850GTS-PWR+:1(config)#access-policy 5 mode allow network
192.192.192.0 24
```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Table 61: Variable definitions

Variable	Value
mode <i><allow deny></i>	Specifies whether a designated network address is allowed or denied access through the specified access service. The default is allow.
network <i><A.B.C.D> <A.B.C.D></i>	The IPv4 address and subnet mask, permitted or denied access through the specified access service.

Configuring access policies by MAC address

About this task

Configure access-policies by MAC address to allow or deny local MAC addresses on the network management port after an access policy is activated. If the source MAC does not match a configured entry, the default action is taken. A log message is generated to record the denial of

access. For connections coming in from a different subnet, the source mac of the last hop is used in decision making. Configure access-policies by MAC address does not perform MAC or Forwarding Database (FDB) filtering on data ports.

Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

2. Add the MAC address and configure the action for the policy:

```
access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>
```

3. Specify the action for a MAC address that does not match the policy:

```
access-policy by-mac action <allow|deny>
```

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1configure terminal
```

Add the MAC address:

```
VSP-4850GTS-PWR+:1(config)#access-policy by-mac 00-C0-D0-86-BB-E7 allow
```

Variable definitions

Use the data in the following table to use the `access-policy by-mac` command.

Table 62: Variable definitions

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00>	Adds a MAC address to the policy. Enter the MAC address in hexadecimal format.
<allow deny>	Specifies the action to take for the MAC address.

System access security enhancements

The section provides information on security enhancements after you enable enhanced secure mode.

Enabling enhanced secure mode

Use the following procedure to enable enhanced secure mode. Enhanced secure mode is disabled by default.

About this task

* Note:

When you migrate your switch from enhanced secure mode enabled to disabled, or from disabled to enabled, you must build a new configuration. Do not use a configuration created in either enhanced secure mode disabled or enabled, and expect it to transfer over to the new mode.

The configuration file cannot be guaranteed if you transfer between enhanced secure mode enabled to disabled, or from enhanced secure mode disabled to enabled.

After you enable the enhanced secure mode, the system provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use. The enhanced secure mode boot flag supports two sub-modes namely JITC and non-JITC.

After you disable enhanced secure mode, the authentication, access-level, and password requirements work similarly to any of the existing commercial releases.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable enhanced secure mode:

```
boot config flags enhancedsecure-mode [jitc | non-jitc]
```

* Note:

It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode, because the JITC sub-mode is more restrictive and prevents the use of some ACLI commands that are commonly used for troubleshooting.

3. **(Optional)** Disable enhanced secure mode:

```
no boot config flags enhancedsecure-mode
```

4. **(Optional)** Configure the enhanced secure mode to the default value:

```
default boot config flags enhancedsecure-mode
```

5. Save the configuration:

```
save config
```

*** Note:**

The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

6. Restart the switch:

```
boot [config WORD<1-99>] [-y]
```

*** Note:**

If you enter the `boot` command with no arguments, you cause the switch to start using the current boot choices defined by the `boot config choice` command.

If you enter a boot command and the configuration filename without the directory, the device uses the configuration file from `/intflash/`.

Example

Enable the enhanced secure non-JITC sub-mode:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags enhancedsecure-mode non-jitc
Switch:1(config)#save config
Switch:1(config)#exit
Switch:1(config)#boot config /intflash/config.cfg -y
```

Enable the enhanced secure JITC sub-mode:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags enhancedsecure-mode jitc
Switch:1(config)#save config
Switch:1(config)#exit
Switch:1(config)#boot config /intflash/config.cfg -y
```

Variable definitions

Use the data in the following table to use the `boot config flags enhancedsecure-mode` command.

Variable	Value
jitc	Enables the JITC enhanced secure mode. The JITC mode is more restrictive and prevents the use of some ACLI commands that are commonly used for troubleshooting.
non-jitc	Enables the non-JITC enhanced secure mode.

Displaying the boot config flags status

Use the following procedure to display the boot config flags status.

If enhanced secure mode is enabled, the status displays whether the JITC or non-JITC sub-mode is enabled. If enhanced secure mode is disabled, the status displays as false.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. View the boot flag status:

```
show boot config flags
```

Example

The status displays the sub-mode in which the enhanced secure mode is enabled, that is, either the JITC or non-JITC. In the following example, the status displays that the non-JITC sub-mode is enabled.

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags enhancedsecure-mode non-jitc
flags factorydefaults false
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode false
flags verify-config true
```

In this example, the enhanced secure mode displays as false, which means the enhanced secure mode is disabled:

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags enhancedsecure-mode false
flags factorydefaults false
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-config-mode true
```

```
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode false
flags verify-config true
```

Creating accounts for different access levels

Use the following procedure to create accounts for different access levels in enhanced secure mode. You must be the administrator to configure the different access levels.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create accounts on the switch for different access levels:

```
password create-user {auditor|operator|privilege|security} WORD<1-255>
```

3. Save the configuration:

```
save config
```

* Note:

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Create an account at the auditor level for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password create-user auditor jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password create-user** command.

Variable	Value
<i>{auditor operator privilege security}</i>	Specifies the access level for the user.
<i>WORD<1–255></i>	Specifies the user name.

Deleting accounts in enhanced secure mode

Use the following procedure to delete accounts in enhanced secure mode.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
- You must be an admin or privilege user to delete accounts.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Delete an account on the switch:

```
password delete-user username WORD<1–255>
```

3. Save the configuration:

```
save config
```

Note:

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Delete an account for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password delete-user user-name jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password delete-user** command.

Variable	Value
<i>user-name WORD<1–255></i>	Specifies the user name.

Configuring a password for a specific user

Configure a new password for a user if the password has expired or locked. Only the administrator can configure a password for a user.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create accounts on the switch for different access levels:

```
password set-password user-name WORD<1-255>
```

3. Save the configuration:

```
save config
```

* Note:

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Configure a password for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password set-password user-name jsmith
Enter the New password : *****
Switch:1(config)#Password modified for user jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password set-password** command.

Variable	Value
user-name <i>WORD<1-255></i>	Specifies the user for which to configure the password.

Returning the system to the factory defaults

Return the system to factory defaults. Reset the switch to the default passwords and configuration. If you use this command, the system returns to factory defaults, returns necessary flags to their default values, and deletes all of the configured user accounts in enhanced secure mode.

You can only access this command after you enable enhanced secure mode. Only the individual with the administrator access role can use this command. After the administrator uses this command, the administrator must reboot the switch.

Note:

The command `sys sys-default` does not save the config file. When you execute the command `sys sys-default`, you must reboot the system to have the command take effect. After the system reboots, you must login and then save the config file. Otherwise, if you reboot the device again for a second time without saving the config file, the changes are not saved and the system comes back up in enhanced secure mode.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
- Save the configuration to a file to retain the configuration settings.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. Return the system to the factory defaults:

```
sys system-default
```
3. Restart the switch:

```
reset
```
4. Save the configuration:

```
save config
```

Example

Return the system to the factory defaults:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#sys system-default
```

```
WARNING: Executing this command returns the system to factory defaults and deletes all
local configured user accounts.
```

System access configuration using ACLI

```
This command needs system reset to take into effect  
Do you want to continue (y/n) ? y
```

```
Switch:1#reset
```

The device reboots and the Admin user logs into the system again.

```
Switch:1(config)#save config
```

Configuring the password complexity rule

About this task

Use the following procedure to configure the password complexity rule.

The password complexity rule default is to use at least two uppercase, two lowercase, two numeric, and two special character to meet the password criteria.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

2. Configure the password complexity rule:

```
password password-rule <1-2> <1-2> <1-2> <1-2>
```

3. **(Optional)** Configure the password complexity rule to the default:

```
default password password-rule
```

4. Save the configuration:

```
save config
```

Note:

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Configure the password complexity rule to require two uppercase, two lowercase, two numeric and two special characters in each password:

```
Switch:1>enable  
Switch:1#configure terminal
```

```
Switch:1(config)#password password-rule 2 2 2 2
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password password-rule` command.

Variable	Value
<1-2> <1-2> <1-2> <1-2>	Configures the minimum password rule. The first variable defines the number of uppercase characters required. The second <1-2> variable defines the number of lowercase characters required. The third <1-2> variable defines the number of numeric characters required. The fourth <1-2> variable defines the number of special characters required. The default for each of these is 2.

Configuring the password length rule

About this task

Configure the password length rule after you enable enhanced secure mode. By default, the minimum password length is 15.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the password length rule option:

```
password min-passwd-len <8-32>
```

3. **(Optional)** Configure the password length rule to the default:

```
default password min-passwd-len
```

4. Save the configuration:

```
save config
```

* Note:

The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the password length rule to 20:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password min-passwd-len 20
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password min-passwd-len` command.

Variable	Value
<8–32>	Configures the minimum character length required. The default is 15.

Configuring the change interval rule

About this task

Use the following procedure to configure the change interval rule. The system enforces a minimum password change interval, which defines the minimum amount of time before you can change to a new password. By default, the minimum change interval is 24 hours between changing from one password to a new password.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:
`enable`
`configure terminal`
2. Configure the change interval rule option:
`password change-interval <1-999 hours>`
3. **(Optional)** Configures the change interval rule to the default:
`default password change-interval`
4. Save the configuration:
`save config`

*** Note:**

The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the change interval rule to 72 hours:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password change-interval 72
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password change-interval` command.

Variable	Value
<1-999>	Configures the minimum interval between consecutive password changes. The default is 24 hours.

Configuring the reuse rule

Use the following procedure to configure the password reuse rule. The default password reuse rule is 3.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

- Enter Global Configuration mode:


```
enable
configure terminal
```
- Configure the password reuse rule option:


```
password password-history <3-32>
```
- (Optional)** Configure the password reuse rule to the default:


```
default password password-history
```
- Save the configuration:


```
save config
```

*** Note:**

The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the reuse rule to 88:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password password-history 30
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password password-history` command.

Variable	Value
<3–32>	Configures the minimum number of previous passwords to remember. The default is 3.

Configuring the maximum age rule

Use the following procedure to configure the maximum age rule.

If enhanced secure mode is enabled, the individual with the administrator access level role can configure the aging-time for each user. If you configure the aging time for each user, the aging time must be more than the global change interval value. The default is 90 days.

If you do not enable enhanced secure mode, the aging time is a global value for all users.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the maximum age rule option:

```
password aging-time day <1-365> [user WORD<1-255>]
```

3. **(Optional)** Configure the maximum age rule to the default:

```
default password aging-time [user WORD<1-255>]
```

4. Save the configuration:

```
save config
```

*** Note:**

The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the maximum age rule option to 100 days for user jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password aging-time day 100 user jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password aging-time` command.

Variable	Value
day <1–365>	Configures the password aging time in days. The default is 90 days.
user <i>WORD</i> <1–255>	Specifies a particular user.

Configuring the maximum number of sessions

Use the following procedure to configure the maximum number of sessions on the switch. The `max-sessions` value configures the number of times a particular role-based user can log in to the switch through the SSH session at the same time. The default `max-sessions` value is 3.

The `max-sessions` value applies only for SSH sessions, and only with enhanced secure mode enabled.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the maximum number of sessions:

```
password max-sessions <1-8> user-name WORD<1-255>
```

3. **(Optional)** Configure the password reuse rule to the default:

```
default password max-sessions
```

4. Save the configuration:

```
save config
```

* **Note:**

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Configure the reuse rule to 5:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password max-sessions 5 user-name jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password max-sessions** command.

Variable	Value
<1-8>	Specifies the maximum number of sessions. The default is 3.
user-name <i>WORD</i> <1-255>	Specifies the user-name.

Configuring the pre- and post-notification rule

Use the following procedure to configure the pre-notification and post-notification rule.

After enhanced secure mode is enabled, the switch enforces password expiry. To ensure a user does not lose access, the switch offers pre- and post-notification messages explaining when the password will expire.

The administrator can define pre- and post-notification intervals to between one to 99 days.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

About this task

The pre-notification intervals provide messages to warn users that their passwords will expire within a particular timeframe:

- interval 1—By default, interval 1 is 30 days.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 1 day.

The post-notification intervals provide notification to users that their passwords have expired within a particular timeframe:

- interval 1—By default, interval 1 is 1 day.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 30 days.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the pre-notification rule option:

```
password pre-expiry-notification-interval <1-99> <1-99> <1-99>
```

3. Configure post-notification rule option:

```
password post-expiry-notification-interval <1-99> <1-99> <1-99>
```

4. Configure the pre-notification rule to the default:

```
default password pre-expiry-notification-interval
```

5. Configure the post-notification rule to the default:

```
default password post-expiry-notification-interval
```

6. Save the configuration:

```
save config
```

* Note:

The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Configure the pre- and post-notification rules to the default:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#default password pre-expiry-notification-interval
Switch:1(config)#default password post-expiry-notification-interval
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **pre-expiry-notification-interval** command.

Variable	Value
<1-99> <1-99> <1-99>	<p>Configure the pre-notification intervals to provide messages to warn the users that their passwords will expire within a particular timeframe.</p> <p>The first <1-99> variable specifies the first notification, the second <1-99> specifies the second notification, and the third <1-99> variable specifies the third interval.</p> <p>By default, the first interval is 30 days, the second interval is 7 days, and the third interval is 1 day.</p>

Use the data in the following table to use the `post-expiry-notification-interval` command.

Variable	Value
<1-99> <1-99> <1-99>	<p>Configure the post-notification intervals to provide notification to the users that their passwords have expired within a particular timeframe.</p> <p>The first <1-99> variable specifies the first notification, the second <1-99> specifies the second notification, and the third <1-99> variable specifies the third interval.</p> <p>By default, the first interval is 1 day, the second interval is 7 days, and the third interval is 30 days.</p>

Chapter 29: System access configuration using EDM

The section provides procedures you can use to manage system access by using Enterprise Device Manager (EDM). Procedures include configurations for usernames, passwords, and access policies.

Configuring CLI access using EDM

Use the following procedures to perform CLI access configuration tasks such as:

- Enable access levels
- Change passwords
- Configure the logon banner

Enabling access levels

About this task

Enable access levels to control the configuration actions of various users.

Important:

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

The system preserves these configurations across restarts.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Select the enable check box for the required access level.
5. Click **Apply**.

Changing passwords

About this task

Configure new passwords for each access level, or change the logon or password for the different access levels of the system to prevent unauthorized access. After you receive the switch, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change passwords in encrypted format.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Specify the username and password for the appropriate access level.
5. Click **Apply**.

Configuring the logon banner

About this task

Configure the logon banner using EDM to display a warning message to users of the CLI before authentication.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Enter the banner text in the **CustomBannerText** field.
5. Check the **CustomBannerEnable** check box.
6. Click **Apply**.

CLI field descriptions

Use the data in the following table to use the **CLI** tab.

Name	Description
RWAUserName	Specifies the user name for the read-write-all CLI account.
RWAPassword	Specifies the password for the read-write-all CLI account.
RWEnable	Activates the read-write access. The default is enabled.
RWUserName	Specifies the user name for the read-write CLI account.

Table continues...

Name	Description
RWPassword	Specifies the password for the read-write CLI account.
RWL3Enable	Activates the read-write Layer 3 access. The default is enabled.
RWL3UserName	Specifies the user name for the Layer 3 read-write CLI account.
RWL3Password	Specifies the password for the Layer 3 read-write CLI account.
RWL2Enable	Activates the read-write Layer 2 access. The default is enabled.
RWL2UserName	Specifies the user name for the Layer 2 read-write CLI account.
RWL2Password	Specifies the password for the Layer 2 read-write CLI account.
RWL1Enable	Activates the read-write Layer 1 access. The default is enabled.
RWL1UserName	Specifies the user name for the Layer 1 read-write CLI account.
RWL1Password	Specifies the password for the Layer 1 read-write CLI account.
ROEnable	Activates the read-only CLI account. The default is enabled.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Specifies the maximum number of concurrent Telnet sessions in a range from 0–8. The default is 8.
MaxRloginSessions	Specifies the maximum number of concurrent Rlogin sessions in a range from 0–8. The default is 8.
Timeout	Specifies the number of seconds of inactivity for a Telnet or Rlogin session before the system initiates automatic timeout and disconnect, expressed in a range from 30–65535. The default is 900 seconds.
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This variable is a read-only field.
CustomBannerText	Specifies the text message that is displayed to users on the CLI before authentication. The message can be company information, such as company name and contact, or a warning message for the users of CLI. With character limitation from 1-1800, the text box displays 79 characters per line.
CustomBannerEnable	Specifies whether custom logon banner is enabled or disabled. The default is enabled.

Creating an access policy

About this task

Create an access policy to control access to the switch. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, SNMP, HTTP, SSH, and rlogin.

You can allow network stations to access the switch or forbid network stations to access the switch. For each service, you can also specify the level of access, such as read-only or read-write-all.

HTTP and HTTPS support IPv4.

 **Important:**

EDM does not provide SNMPv3 support for an access policy. If you modify an access policy with EDM, SNMPV3 is disabled.

Procedure

1. In the navigation tree, open the following folders: **Configuration > Security > Control Path**.
2. Click **Access Policies**.
3. Click the **Access Policies** tab.
4. Click **Insert**.
5. In the **ID** box, type the policy ID.
6. In the **Name** box, type the policy name.
7. Select the **PolicyEnable** check box.
8. Select the **Mode** option to allow or deny a service.

If you configure the access policy mode to **deny**, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to **deny**, the system does not check **AccessLevel** or **AccessStrict** information. If you configure the access policy mode to allow, the system continues to check the **AccessLevel** and **AccessStrict** information.

9. From the **Service** options, select a service.
10. In the **Precedence** box, type a precedence number for the service (lower numbers mean higher precedence).
11. Select the **NetInetAddressType**.
12. In the **NetInetAddress** box, type an IP address.
13. In the **NetInetAddressPrefixLen** box, type the prefix length.
14. In the **TrustedHostInetAddress** box, type an IP address for the trusted host.
15. In the **TrustedHostUserName** box, type a user name for the trusted host.
16. Select an **AccessLevel** for the service.
17. Select the **AccessStrict** check box, if required.

 **Important:**

If you select the **AccessStrict** option, you specify that a user must use an access level identical to the one you select.

18. Click **Insert**.

Access Policies field descriptions

Use the data in the following table to use the **Access Policies** tab.

Name	Description
Id	Specifies the policy ID.
Name	Specifies the name of the policy.
PolicyEnable	Activates the access policy. The default is enabled.
Mode	<p>Indicates whether a packet with a source IP address matching this entry is permitted to enter the device or is denied access. The default is allow.</p> <p>If you configure the access policy mode to deny, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to deny, the system does not check AccessLevel or AccessStrict information. If you configure the access policy mode to allow, the system continues to check the AccessLevel and AccessStrict information.</p>
Service	Indicates the protocol to which this entry applies. The default is no service enabled.
Precedence	Indicates the precedence of the policy expressed in a range from 1–128. The lower the number, the higher the precedence. The default is 10.
NetInetAddrType	<p>Indicates the source network Internet address type as one of the following.</p> <ul style="list-style-type: none"> • any • IPv4 <p>IPv4 is expressed in the format a.b.c.d.</p>
NetInetAddress	Indicates the source network Inet address (prefix/network). If the address type is IPv4, you must enter an IPv4 address and its mask length. You do not need to provide this information if you select the NetInetAddrType of any.
NetInetAddrPrefixLen	Indicates the source network Inet address prefix-length/mask. If the type is IPv4, you must enter an IPv4 address and mask length. You do not need to provide this information if you select the NetInetAddrType of any.
TrustedHostInetAddr	Indicates the trusted Inet address of a host performing a remote login to the device. You do not need to provide this information if you select the NetInetAddrType of any. TrustedHostInetAddr applies only to rlogin and rsh.

Table continues...

Name	Description
	<p>! Important:</p> <p>You cannot use wildcard entries in the TrustedHostInetAddr field.</p> <p>If the type is IPv4, you must enter an IPv4 address and mask length.</p>
TrustedHostUserName	<p>Specifies the user name assigned to the trusted host. The trusted host name applies only to rlogin and rsh. Ensure that the trusted host user name is the same as your network logon user name; do not use the switch user name, for example, rwa.</p> <p>! Important:</p> <p>You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. For example, using "rlogin -l newusername xx.xx.xx.xx" does not work from a UNIX workstation.</p>
AccessLevel	<p>Specifies the access level of the trusted host as one of the following:</p> <ul style="list-style-type: none"> • readOnly • readWrite • readWriteAll <p>The default is readOnly.</p>
Usage	<p>Counts the number of times this access policy applies.</p>
AccessStrict	<p>Activates or disables strict access criteria for remote users.</p> <p>If selected, a user must use an access level identical to the one you selected in the dialog box to use this service.</p> <ul style="list-style-type: none"> • selected: remote login users can use only the currently configured access level • cleared: remote users can use all access levels <p>! Important:</p> <p>If you do not select true or false, user access is governed by criteria specified in the policy table. For example, a user with an rw access level specified for a policy ID in the policy table is allowed rw access, and ro is denied access.</p> <p>The default is false.</p>

Enabling an access policy

About this task

Enable the access policy feature globally to control access across the switch.

You can create an access policy to control access to the switch. An access policy specifies the hosts or networks that can access the switch through access services; for example Telnet, SNMP, Hypertext Transfer Protocol (HTTP), and remote login (rlogin).

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, expand the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. Select the **EnableAccessPolicy** check box.
6. Click **Apply**.
7. Click **Close**.

System access security enhancements using EDM

The section provides information to enable enhanced secure mode.

Enabling enhanced secure mode

Use the following procedure to enable enhanced secure mode in either the JITC or non-JITC sub-modes.

The enhanced secure mode is disabled by default.

About this task

After you enable enhanced secure mode, the system can provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.

After you disable enhanced secure mode, the authentication, access-level, and password requirements work similarly to any of the existing commercial releases.

Note:

You can use EDM to enable or disable enhanced secure mode. To configure the security enhancements this feature provides, you must use ACLI.

Procedure

1. On the Device Physical View, select the device.
2. In the navigation pane, expand the following folders: **Configuration > Edit**
3. Click **Chassis**.
4. Click the **Boot Config** tab.
5. In the **EnableEnhancedsecureMode** option box, select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. Select **disable** to disable the enhanced secure mode.

 **Note:**

It is recommended that you enable the non-JITC sub-mode. The JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

6. Click **Apply**.
7. Save the configuration, and restart the switch.

Chapter 30: ACLI show command reference

This reference information provides show commands to view the operational status of the Avaya Virtual Services Platform 4000 Series.

Access, logon names, and passwords

Use the `show cli password` command to display the access, logon name, and password combinations. The syntax for this command is as follows.

show cli password

The following example shows output from the `show cli password` command if enhanced secure mode is disabled.

```
Switch:1#show cli password
  access-level
  aging      90

  min-passwd-len 10
  password-history 3

  ACCESS      LOGIN      STATE
  rwa         rwa         NA
  rw          rw         ena
  13         13         ena
  12         12         ena
  11         11         ena
  ro          ro         ena
  Default Lockout Time      60
  Lockout-Time:
                IP                Time
```

The following example shows output from the `show cli password` command if enhanced secure mode is enabled.

*** Note:**

After you enable enhanced secure mode, the parameters in the output for the `show cli password` command apply to all of the role-based users, except for the admin user. So for instance, the system mandates that the admin user must have a password length of 15, and a password with two of each of the following characters: uppercase, lowercase, numeric and special character. However, the admin user can then configure this differently for the other user access levels. The following values that display for min-passwd-len and password-rule are

those configured by admin, and they apply to the privilege, operator, security, and auditor access levels.

```
Switch:1#show cli password
  change-interval 24
  min-passwd-len 8
  password-history 3
  password-rule 1 1 1 1
  pre-expiry-notification-interval 1 7 30
  post-expiry-notification-interval 1 7 30
  access-level
  ACCESS      LOGIN      AGING  MAX-SSH-SESSIONS  STATE
  admin       rwa          90    3                  ena
  privilege   oper1        90    3                  dis
  operator    oper1        90    3                  ena
  security    security     90    3                  ena
  auditor     auditor      90    3                  ena
  Default Lockout Time      60
  Lockout-Time:
```

Basic switch configuration

Use the **show basic config** command to display the basic switch configuration. The syntax for this command is as follows.

show basic config

The following example shows the output of this command.

```
VSP-4850GTS-PWR+:1#show basic config
  setdate : N/A
  auto-recover-delay : 30
```

Current switch configuration

Use the **show running-config** command to display the current switch configuration. The syntax for this command is as follows.

show running-config [verbose] [module <boot|cfm|cli|diag|fa|fhs|filter|ip|ipsec|ipv6|isis|lcp|lldp|macsec|mlt|naap|nsna|ntp|poe|port|qos|radius|rmon|slamon|slpp|spbm|stg|sys|tacacs|vlan|web>]

The following table explains parameters for this command.

Table 63: Command parameters

Parameter	Description
module	Specifies the command group for which you request configuration settings.

Table continues...

Parameter	Description
<boot cfm cli diag fa fhs filter ip ipsec ipv6 isis lacp lldp macsec mlt naap nsna ntp poe port qos radius rmon slamon slpp spbm stg sys tacacs vlan web>	
verbose	Specifies a complete list of all configuration information about the switch.

If you make a change to the switch, it appears under the specific configuration heading. The following example shows a subset of the output of this command.

```
VSP-4850GTS-PWR+:1#show running-config
Preparing to Display Configuration...
#
# Sat Jan 04 14:04:23 2014 UTC
# box type           : VSP-4850GTS-PWR+
# software version   : vsp4k_4.1.0.0_B017 (PRIVATE)
# cli mode           : ACLI      #
--More-- (q = quit)
```

* Note:

The output of the `show running-config` command displays `end` near the end of the configuration status. This means that the script is exiting the Global Configuration mode and loading the rest of the configuration in Privileged EXEC mode, which is a requirement when loading the IP redistribution commands.

If you add `verbose` to the `show running-config` command, the output contains current switch configuration including software (versions), performance, VLANs (numbers, port members), ports (type, status), routes, memory, interface, and log and trace files. With the verbose command, you can view the current configuration and default values.

CLI settings

Use the `show cli info` command to display information about the ACLI configuration. The syntax for this command is as follows.

`show cli info`

The following example shows sample output from the `show cli info` command.

```
VSP-4850GTS-PWR+:1#show cli info

cli configuration

ore                : true
screen-lines       : 23
telnet-sessions    : 8
rlogin-sessions    : 8
timeout            : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt : true
default login prompt   : Login:
```

```

custom login prompt      : Login:
use default password prompt : true
default password prompt  : Password:
custom password prompt   : Password:
prompt : VSP-4850GTS-PWR+
    
```

Ftp-access sessions

Use the **show ftp-access** command to display the total sessions allowed. The syntax for this command is as follows.

show ftp-access

The following example shows output from the **show ftp-access** command.

```

VSP-4850GTS-PWR+:1#show ftp-access
max ipv4 sessions : 4
    
```

Hardware information

Use the **show sys-info** command to display system status and technical information about the switch hardware components. The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information. The syntax for this command is as follows.

show sys-info [card] [fan] [led] [power] [usb]

The following table explains parameters for this command.

Table 64: Command parameters

Parameter	Description
card	Specifies information about the device. Includes type, serial number and assembly date.
fan	Specifies information about installed cooling modules.
led	Displays LED information in detail.
power	Specifies information about installed power supplies.
usb	Specifies information about the USB.

The following example shows partial output from the **show sys-info** command.

```

VSP4K-219:1#show sys-info
General Info :
SysDescr      : VSP-4850GTS-PWR+ (4.1.0.0) HW Base: VSP 4850
    
```

```

SysName       : VSP4K-219
SysUpTime    : 6 day(s), 14:11:08
SysContact   : http://support.avaya.com/
SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 07920

```

Chassis Info:

```

Chassis       : 4850GTS-PWR+
Serial#      : 13JP245V901R
H/W Revision  : 10
H/W Config   : none
NumSlots     : 1
NumPorts     : 50
BaseMacAddr  : b4:a9:5a:2d:6c:00
MacAddrCapacity : 256
Temperature  : 31
System MTU   : 9600

```

Card Info :

Slot#	CardType	Serial#	Part#	Oper Status	Admin Status	Power State
1	4850GTS-PWR+	13JP245V901R	--	up	up	on

Power Supply Info :

```

Ps#1 Status   : up
Ps#1 Type     : AC
Ps#1 Description : 4850GTS-PWR+
Ps#1 Serial Number: LBNTTMDT201ERGT
Ps#1 Version  : --
Ps#1 Part Number : 325220-A.01

Ps#2 Status   : empty

Total Power Available : 1000 watts
Total Power Usage    : 145 watts

```

Fan Info :

```

Fan#1 Status       : up
Fan#1 AmbientTemperature : 31
Fan#1 Type         : regularSpeed

Fan#2 Status       : up
Fan#2 AmbientTemperature : 31

```

```

Fan#2 Type           : regularSpeed

Fan#3 Status        : up
Fan#3 AmbientTemperature : 31
Fan#3 Type          : regularSpeed

LED Info :

LED#1 Label  : PWR
LED#1 Status : GreenSteady

LED#2 Label  : Status
LED#2 Status : GreenSteady

LED#3 Label  : Rps
LED#3 Status : Off

LED#4 Label  : Up
LED#4 Status : UnSupported

LED#5 Label  : Down
LED#5 Status : UnSupported

LED#6 Label  : Base
LED#6 Status : UnSupported

```

Use **show interface gigabitEthernet** command to display the port information of the VSP 4000 switch. The syntax to this command is as follows:

show interface gigabitEthernet {[slot/port][slot/port][...]}

*** Note:**

Ports 47 and 48 are the combo ports and they support both copper and fiber on the same switch port. Combo port SFP slot supports Avaya 1G SFPs and 100Base low speed SFPs and SFP+ slot supports Avaya’s 1G SFPs and 10G SFP+s.

Following example shows output from **show interfaces gigabitEthernet 1/47 - 1/48** command:

```

VSP4K-219:1#show interfaces gigabitEthernet 1/47-1/48

=====
                        Port Interface
=====
PORT      LINK  PORT      PHYSICAL      STATUS
NUM  INDEX DESCRIPTION  TRAP  LOCK  MTU  ADDRESS      ADMIN  OPERATE

```

```

-----
1/47 238 GbicSx      true false 9600 b4:a9:5a:2d:6c:2e up   down
1/48 239 GbicSx      true false 9600 b4:a9:5a:2d:6c:2f up   down
-----

Port Name
-----
PORT      OPERATE  OPERATE  OPERATE
NUM  NAME      DESCRIPTION  STATUS  DUPLX  SPEED  VLAN
-----
1/47      GbicSx      down     half    0      Tagged
1/48      GbicSx      down     half    0      Tagged
-----

Port Config
-----
PORT      DIFF-SERV  QOS  MLT  VENDOR
NUM  TYPE      EN   TYPE LVL  ID   NAME
-----
1/47  GbicSx    true core 1    0    Avaya
1/48  GbicSx    true core 1    0    Avaya

PORT  ADMIN  OPERATE  AUTO  ACCESS-SERV
NUM  ROUTING  ROUTING  RECOVER  EN
-----
1/47  Enable  Disable  Disable  FALSE
1/48  Enable  Disable  Disable  FALSE
-----

Port Config L1
-----
PORT  AUTO  CUSTOM AUTO NEGOTIATION  ADMIN  OPERATE  TX-FLW
NUM  NEG.  ADVERTISEMENTS          DPLX  SPD  DPLX  SPD  CONTRL
-----
1/47  true  Not Configured          full 1000  0  disable
1/48  true  Not Configured          full 1000  0  disable

--More-- (q = quit)

```

NTP server statistics

Use the `show ntp statistics` command to view the following information:

- number of NTP requests sent to this NTP server
- number of times this NTP server updated the time
- number of times the client rejected this NTP server while attempting to update the time
- stratum
- version
- sync status
- reachability

- root delay
- precision

The syntax for this command is as follows.

show ntp statistics

The following example shows sample command output.

```
VSP-4850GTS-PWR+:1##show ntp statistics
N      NTP Server : 192.0.2.187
-----
          Stratum : unknown
          Version : unknown
          Sync Status : unknown
          Reachability : unknown
          Root Delay : unknown
          Precision : unknown
          Access Attempts : 0
          Server Synch : 0
          Server Fail : 0
          Fail Reason : unknown
```

Power summary

Use the **show sys power** command to view a summary of the power information for the chassis.

The syntax for this command is as follows.

show sys power [global] [power-supply] [slot]

The following example shows sample command output.

```
VSP-4850GTS-PWR+:1##show sys power
=====
                          Chassis Power Information
=====

Chassis Power Status: non-redundant

          Total      Required  Max
Chassis Chassis  Redundant Allocated Available
Type   Power      Power      Power      Power
-----
4850GTS-PWR+ 1000      0          145      855
-----
```

Power information for power supplies

Use the **show sys power power-supply** command to view detailed power information for each power supply.

The syntax for this command is as follows.

show sys power power-supply

The following example shows sample command output.

```
VSP-4850GTS-PWR+:1#show sys power power-supply
```

```
=====
Power Supply Information
=====
Power  Type      Input  Serial      Part      Oper   Max
Supply                Voltage Num        Num              Status Power
-----
PS#1   AC          220    LBNNTMDT200NEVT 325220-A.01    up     1000
=====
```

System information

Use the **show sys** command to display system status and technical information about the switch hardware components and software configuration. The command shows several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information. The syntax for this command is as follows.

show sys <dns|force-msg|mgid-usage|msg-control|mtu|power|setting|software|stats|topology-ip>

The following table explains parameters for this command.

Table 65: Command parameters

Parameter	Description
dns	Shows the DNS default domain name.
force-msg	Shows the message control force message pattern settings.
mgid-usage	Shows the multicast group ID (MGID) usage for VLANs and multicast traffic.
msg-control	Shows the system message control function status (activated or disabled).
mtu	Shows system maximum transmission unit (MTU) information.
power	Shows power information for the chassis. Command options are <ul style="list-style-type: none"> • power-supply—power information for each power supply • slot—power information for each slot

Table continues...

Parameter	Description
setting	Shows system settings.
software	Shows the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags.
stats	Shows system statistics. For more information about statistics, see <i>Performance Management of Avaya Virtual Services Platform 4000 Series</i> , NN46251-701.
topology-ip	Shows the circuitless IP set.

The following example shows output from the **show sys dns** command.

```
VSP-4850GTS-PWR+:1#show sys dns
```

The following example shows output from the **show sys mgid-usage** command.

```
VSP-4850GTS-PWR+:1#show sys mgid-usag
  Number of MGIDs used for VLANs : (6)
  Number of MGIDs used for multicast : (0)
  Number of MGIDs used for SPBM : (0)
  Number of MGIDs remaining for VLANs : (4089)
  Number of MGIDs remaining for multicast : (6976)
  Number of MGIDs remaining for SPBM : (1024)
```

The following example shows output from the **show sys msg-control** command.

```
VSP-4850GTS-PWR+:1#show sys msg-control

Message Control Info :
  action                : suppress-msg
  control-interval      : 5
  max-msg-num           : 5
  status                : disable
```

The following example shows output from the **show sys setting** command.

```
VSP-4850GTS-PWR+:1#show sys setting
  udp-checksum          : enable
  mroute-stream-limit   : disable
  contact               : http://support.avaya.com/
  location              : 211 Mt. Airy Road,Basking Ridge,NJ 07920
  name                  : VSP-4850GTS-PWR+
  portlock              : off
  sendAuthenticationTrap : false
  autotopology          : on
  ForceTopologyIpFlag   : false
  clipId-topology-ip    : 0
  mtu                   : 9600
  prototype             : disable
```

The following example shows output from the **show sys software** command.

```
VSP-4850GTS-PWR+:1#show sys software

System Software Info :
Default Runtime Config File : /intflash/soak1.cfg
```



```

Config File :
Last Runtime Config Save : 0

Boot Config Table
Version : Build 4.1.0.0 (GA) on Fri May 30 18:04:13 EDT 2014
PrimaryConfigSource : /intflash/soak.cfg
SecondaryConfigSource : /intflash/config.cfg
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : false
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : true

```

System status (detailed)

Use the **show tech** command to display technical information about system status and information about the hardware, software, and operation of the switch.

The information available from the **show tech** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), OSPF (area, interface, neighbors), Virtual Router Redundancy Protocol (VRRP), Routing Information Protocol (RIP), and log and trace files. This command displays more information than the similar **show sys-info** command. The syntax for this command is as follows.

show tech

The following example shows representative output from the **show tech** command.

```

VSP-4450GSX-PWR+:1#show tech

Sys Info:
-----

General Info :

    SysDescr      : VSP-4450GSX-PWR+ (4.1.0.0) (GA)  HW Base: VSP 4450
    SysName       : VSP4K-38
    SysUpTime     : 7 day(s), 22:32:54
    SysContact    : http://support.avaya.com/
    SysLocation   : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

    Chassis       : 4450GSX-PWR+
    Serial#       : SDNIV50S1020
    H/W Revision  : 1
    H/W Config    : R0B
    NumSlots      : 1
    NumPorts      : 50
    BaseMacAddr   : f8:15:47:e1:73:00
    MacAddrCapacity : 256

```

```
--More-- (q = quit)
```

Telnet-access sessions

Use the **show telnet-access** command to display to show the total sessions allowed. The syntax for this command is as follows.

show telnet-access

The following example shows output from the **show telnet-access** command.

```
VSP-4850GTS-PWR+:1#show telnet-access
max ipv4 sessions : 8
```

Users logged on

Use the **show users** command to display a list of users currently logged on to the system. The syntax for this command is as follows.

show users

The following example shows output from the **show users** command.

```
VSP-4850GTS-PWR+:1#show users
SESSION  USER          ACCESS  IP ADDRESS
Telnet0  rwa           rwa     192.0.2.24 (current)
Console  none         none     -----
```

Port egress COS queue statistics

Use the **show qos cosq-stats interface <PT_PORT>** to retrieve the port egress COS queue statistics. The syntax for this command is as follows:

show qos cosq-stats interface <PT_PORT>

The following example shows output from the **show qos cosq-stats interface <PT_PORT>** command.

```
VSP38:1#show qos cosq-stats interface 1/46
=====
Port:1/46  QOS CoS Queue Stats
=====
CoS  Out Packets      Out Bytes      Drop Packets      Drop Bytes
-----
0    13144            841216         0                 0
```

```

1      0      0      0      0
2      0      0      0      0
3      0      0      0      0
4      0      0      0      0
5      0      0      0      0
6  36964  6394746  0      0
7      0      0      0      0
VSP38:1#

```

CPU queue statistics

Use the `show qos cosq-stats cpu-port` to display the statistics of the forwarded packets and bytes, and the dropped packets and bytes for the traffic sent toward CP. The queue assignment is based on the protocol types, not on the internal COS value. These statistics are useful for debugging purposes.

The syntax for this command is as follows:

```
show qos cosq-stats cpu-port
```

The following example shows output from the `show qos cosq-stats cpu-port` command.

```
VSP38:1#show qos cosq-stats cpu-port
```

```

=====
                        QoS CoS Queue Cpu Port Stats Table
=====
CoS   Out Packets      Out Bytes      Drop Packets      Drop Bytes
-----
0      0                  0              0                 0
1      0                  0              0                 0
2      0                  0              0                 0
3      0                  0              0                 0
4      0                  0              0                 0
5      0                  0              0                 0
6      414              35714          0                 0
7      0                  0              0                 0
8      561              41738          0                 0
9      28740            1969460        0                 0
10     12005            2006662        0                 0
11     0                  0              0                 0
12     0                  0              0                 0
13     0                  0              0                 0
14     7280             495040         0                 0
15     0                  0              0                 0

```

Chapter 31: Port numbering and MAC address assignment reference

This section provides information about the port numbering and Media Access Control (MAC) address assignment used on Avaya Virtual Services Platform 4000 Series.

Port numbering

A port number includes the slot location of the module in the chassis, as well as the port position. The following diagrams illustrate the components on the front panels of the Avaya VSP 4000 switches.



Figure 8: VSP 4850GTS

1. VSP 4000 USB cover
2. Switch LEDs
3. 10/100/1000 ports (LEDs above ports)
4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.
5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.
6. Console Port

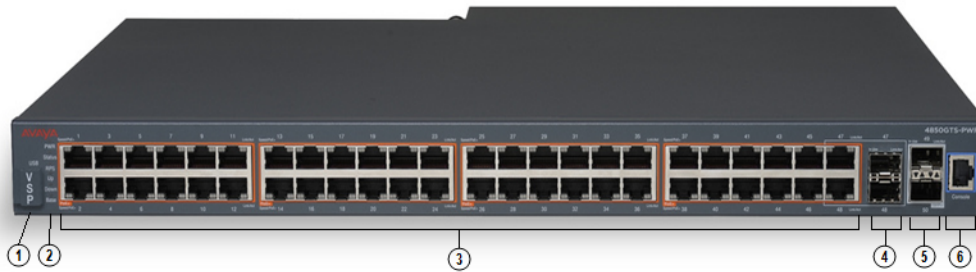


Figure 9: VSP 4850GTS-PWR+

1. VSP 4000 USB cover
2. Switch LEDs
3. 10/100/1000 PoE+ ports (LEDs above ports)
4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.
5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.
6. Console Port

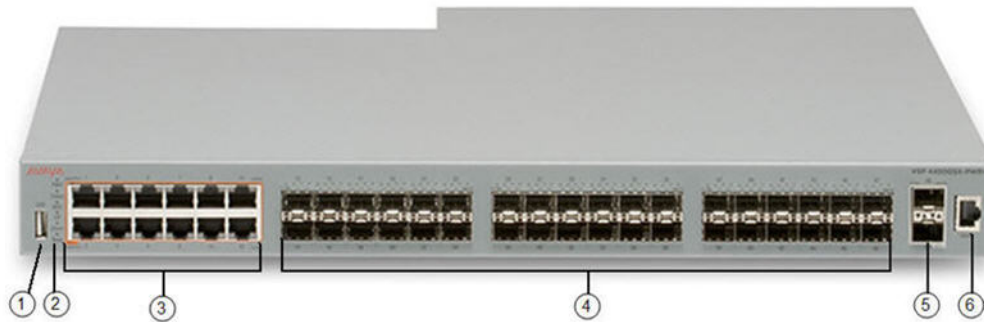


Figure 10: VSP 4450GSX-PWR+

1. VSP 4000 USB port
2. Switch LEDs
3. 10/100/1000 Base TX RJ-45 ports with PoE+ (LEDs above ports)
4. 100/1000 Mbps SFP transceiver modules
5. 1/10G SFP + ports
6. Console Port

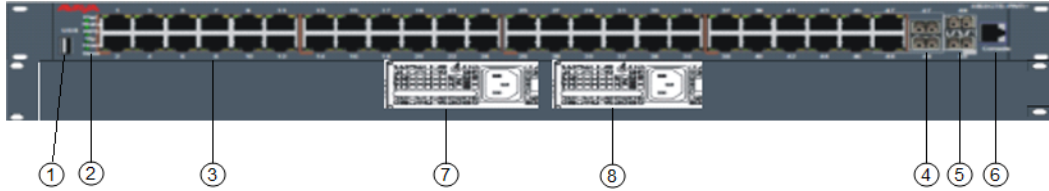


Figure 11: VSP 4450GTX-HT-PWR+

1. VSP 4000 USB port but without a USB or a USB device cover

*** Note:**

The VSP 4450GTX-HT-PWR+ model does not require a USB device in the USB port for normal operation. The USB port can be used for additional storage using a USB memory stick.

2. Switch LEDs

3. 10/100/1000 Base TX RJ-45 ports with 802.3at PoE+

4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs

5. SFP+ slots. Supports Avaya 1G SFPs and 10G SFP+s

6. Console Port

7. Field-replaceable 1000W AC power supply unit (PSU)

8. Second field-replaceable AC power supply unit for redundancy or additional PoE



Figure 12: VSP 4450GSX-DC

1. VSP 4000 USB cover

2. Switch LEDs

3. 10/100/1000 ports (LEDs above ports)

4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.

5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.

6. Console Port

Interface indexes

The Simple Network Management Protocol (SNMP) uses interface indexes to identify ports, Virtual Local Area Networks (VLAN), and Multilink Trunking (MLT).

Port interface index

The interface index of a port is computed using the following formula:

$$\text{ifIndex} = (192 \times \text{slot number}) + (\text{port number} - 1)$$

Slot number is 1.

Port number is a value between 1–50, inclusive.

For example, the interface index of port 1/50 is 241.

VLAN interface index

The interface index of a VLAN is computed using the following formula:

$$\text{ifIndex} = 2048 + \text{VLAN multicast group ID (MGID)}$$

Because the default VLAN always uses an MGID value of 1, its interface index is always 2049.

MLT interface index

The interface index of a multilink trunk (MLT) is computed using the following formula:

$$\text{ifIndex} = 6143 + \text{MLT ID number}$$

MAC address assignment

You must understand MAC addresses assignment if you perform one of the following actions:

- Define static Address Resolution Protocol (ARP) entries for IP addresses in the switch
- Use a network analyzer to decode network traffic

Each chassis is assigned a base of 256 MAC addresses. The first 128 are reserved and the other 128::

- are assigned to routable VLANs. The following figure shows the generic format of a VSP4K MAC address

The MAC address is divided into the following parts:

- Bits 47–24: Institute of Electrical and Electronics Engineers (IEEE) Organization Unique Identity (OUI) (for example, 00-E0-16)
- Bits 23–8: Chassis ID
- Bit 7: 0 port MAC, 1 VLAN MAC
- Bits 6–0: 128 port or VLAN MACs

The base MAC address is derived from the chassis. The MAC Addresses of the ports are based on absolute value and range is 0x01-0x32 VLANs.

Virtual MAC addresses

Virtual MAC addresses are the addresses assigned to VLANs. The system assigns a virtual MAC address to a VLAN when it creates the VLAN. The MAC address for a VLAN IP address is the virtual MAC address assigned to the VLAN.

Chapter 32: Supported standards, RFCs, and MIBs

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that the switch supports.

Supported IEEE standards

The following table details the IEEE standards that the switch supports.

Table 66: Supported IEEE standards

IEEE standard	Description
802.1ag	Connectivity Fault Management
802.1ah	Provider Backbone Bridging
802.1aq	Shortest Path Bridging (SPB)
802.1AX	Link Aggregation
802.1D	MAC Bridges
P802.1p	Traffic Class Expediting & Dynamic Multicast Filtering
802.1Q	Virtual LANs
802.1s	Multiple Spanning Trees
802.1t	802.1D Technical & Editorial Corrections
802.1w	Rapid Spanning Tree Protocol (RSTP)
802.1X-2010	Port-based NAC
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Eletrotechnical Commission (IEC) 8802-3
802.3ab	1000Mb/s Operation, implemented as 1000BASE-T Copper
802.1AE	MAC Security

Table continues...

IEEE standard	Description
802.3ae	10Gb/s Operation, implemented as 10GBASE-X SFP+
802.3ba	40Gb/s and 100Gb/s Operation, implemented as 40GBASE-QSFP+
802.3x	Full Duplex & Flow Control
802.3z	1000Mb/s Operation, implemented as 1000BASE-X SFP

Supported RFCs

The following table and sections list the RFCs that the switch supports.

Table 67: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC 768	UDP Protocol
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet protocol
RFC 894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion control in IP/TCP internetworks
RFC 906	Bootstrap loading using TFTP
RFC 950	Internet Standard Subnetting Procedure
RFC 951	BootP
RFC 959, RFC 1350, and RFC 2428	FTP and TFTP client and server
RFC 1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC 1058	RIPv1 Protocol
RFC 1112	Host Extensions for IP Multicasting (IGMPv1)
RFC 1122	Requirements for Internet Hosts
RFC 1253	OSPF MIB

Table continues...

Request for comment	Description
RFC 1256	ICMP Router Discovery
RFC 1258	IPv6 Rlogin server
RFC 1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC 1340	Assigned Numbers
RFC 1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC 1541	Dynamic Host Configuration Protocol
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 1587	The OSPF NSSA Option
RFC 1591	DNS Client
RFC 1723	RIP v2 — Carrying Additional Information
RFC 1812	Router requirements
RFC 1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC 1981	Path MTU discovery
RFC 2068	Hypertext Transfer Protocol
RFC 2080	RIP
RFC 2131	Dynamic Host Control Protocol (DHCP)
RFC 2138	RADIUS Authentication
RFC 2139	RADIUS Accounting
RFC 2178	OSPF MD5 cryptographic authentication / OSPFv2
RFC 2236	IGMPv2 Snooping
RFC 2284	PPP Extensible Authentication Protocol
RFC 2328	OSPFv2
RFC 2338	VRRP: Virtual Redundancy Router Protocol
RFC 2362	PIM-SM
RFC 2407	IP Security Domain Interpretation of Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2408	Internet Security Associations and Key Management Protocol (ISAKMP)
RFC 2453	RIPv2 Protocol
RFC 2460	IPv6 base stack
RFC 2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Table continues...

Request for comment	Description
RFC 2464	Transmission of IPv6 packets over Ethernet networks
RFC 2545	Use of BGP-4 multi-protocol extensions for IPv6 inter-domain routing
RFC 2548	Microsoft vendor specific RADIUS attributes
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance Statements for SMI v2
RFC 2616	Hypertext Transfer Protocol 1.1
RFC 2710	Multicast Listener Discovery (MLD) for IPv6
RFC 2716	PPP EAP Transport Level Security (TLS) Authentication Protocol
RFC 2819	RMON
RFC 2865	RADIUS
RFC 2874	DNS Extensions for IPv6
RFC 2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC 3046	DHCP Option 82
RFC 3162	IPv6 RADIUS client
RFC 3246	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3315	IPv6 DHCP Relay
RFC 3376	IGMPv3
RFC 3411 and RFC 2418	SNMP over IPv6 networks
RFC 3417	Transport Mappings for SNMP
RFC 3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC 3569	An overview of Source-Specific Multicast (SSM)
RFC 3579	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 3587	IPv6 Global Unicast Address Format
RFC 3748	Extensible Authentication Protocol
RFC 3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP
RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4007	IPv6 Scoped Address Architecture
RFC 4213	IPv6 configured tunnel
RFC 4250–RFC 4256	SSH server and client support
RFC 4291	IPv6 Addressing Architecture
RFC 4301	Security Architecture for IPv6

Table continues...

Request for comment	Description
RFC 4302	IP Authentication Header (AH)
RFC 4303	IP Encapsulated Security Payload (ESP)
RFC 4305	Cryptographic algorithm implementation requirements for ESP and AH
RFC 4308	Cryptographic suites for Internet Protocol Security (IPsec)
RFC 4443	ICMP for IPv6
RFC 4541	Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping
RFC 4552	OSPFv3 Authentication and confidentiality for OSPFv3
RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM)
RFC 4607	Source-Specific Multicast (SSM)
RFC 4835	Cryptographic algorithm implementation for ESP and AH
RFC 4861	IPv6 Neighbor discovery
RFC 4862	IPv6 stateless address autoconfiguration
RFC 5095	Deprecation of Type 0 Routing headers in IPv6
RFC 5187	OSPFv3 Graceful Restart (helper-mode only)
RFC 5340	OSPF for IPv6
RFC 5798	Virtual Router Redundancy Protocol version 3
RFC 6105	IPv6 Router Advertisement Guard
RFC 6329	IS-IS Extensions supporting Shortest Path Bridging
RFC 7610	DHCPv6 Shield

Quality of service

Table 68: Supported request for comments

Request for comment	Description
RFC2474 and RFC2475	DiffServ Support
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB

Network management

Table 69: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (Revision 2)
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2428	FTP Extensions for IPv6
RFC2541	DNS Security Operational Considerations
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2616	IPv6 HTTP server
RFC2819	Remote Network Monitoring Management Information Base
RFC 3411	Architecture for describing SNMP Management Frameworks
RFC4292	IP Forwarding Table MIB

MIBs

Table 70: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657	BGP-4 MIB using SMIv2
RFC2021	RMON MIB using SMIv2
RFC2452	IPv6 MIB: TCP MIB
RFC2454	IPv6 MIB: UDP MIB
RFC2466	IPv6 MIB: ICMPv6 Group
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)
RFC4292	IP Forwarding Table MIB
RFC4363	Bridges with Traffic MIB

Standard MIBs

The following table details the standard MIBs that the switch supports.

Table 71: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib

Table continues...

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934	rfc2934.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control protocol (TCP)	RFC4022	rfc4022.mib


Table continues...

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STD MIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
Q-BRIDGE-MIB —Management Information Base for managing Virtual Bridged LANs	RFC4363	rfc4363-q.mib

Proprietary MIBs

The following table details the proprietary MIBs that the switch supports.

Table 72: Proprietary MIBs

Proprietary MIB name	File name
Avaya IGMP MIB	rfc_igmp.mib
Avaya IP Multicast MIB	ipmroute_rcc.mib
Avaya MIB definitions	wf_com.mib
Avaya PIM MIB	pim-rcc.mib
Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Avaya SLA Monitor Agent MIB	slamon.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5emt103.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definition for Combo Ports	s5ifx.mib
Other SynOptics definition for PoE	bayStackPethExt.mib
Rapid City MIB	rapid_city.mib
 Note: The MACsec tables, namely, rcMACSecCATable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	
SynOptics Root MIB	synro.mib