Administration
Avaya Virtual Services Platform 9000

Release 3.3
NN46250-600
Issue 04.03
June 2013

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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”).

License types

Designated System(s) License (DS). End User may install and use each copy 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, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security

vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Purpose of this document

Administration 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.

Administration supports tasks related to the administration of the network including configuration and management of systems, data, and users. It also includes management of resources and administration tasks on both an initial and ongoing basis.

Chapter 2: New in this release

The following sections detail what is new in *Avaya Virtual Services Platform 9000 Administration*, NN46250–600, for Release 3.3.

Features

See the following sections for information about feature changes.

High Availability

Information on High Availability-CPU mode is updated to include Shortest Path Bridging MAC (SPBM). For more information, see: High Availability-CPU mode on page 85.

Licensed feature content

Shortest Path Bridging MAC (SPBM) is added to the premier license. The premier license activates all features on Virtual Services Platform 9000. For more information, see: Feature licensing on page 155.

SSL certificates

Beginning with this release, you can upload your own certificates to Virtual Services Platform 9000. For more information, see SSL certificates on page 199.

Other changes

See the following section for updates that are not feature-related.

Documentation updates

The following section is updated:

- Port numbering on page 277.

Cooling modules

The model names for cooling modules are updated in software and documentation. For more information, see:

- Hardware and software compatibility on page 87
- Hardware information on page 266
- Slot power details on page 270

Redundant power supplies

Power management on page 89 is updated to explain power supply use in a redundant configuration.

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 9000 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 *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

Where mentioned, configuration files are ASCII text files that allow an administrator to change switch configuration quickly.

Saving the configuration

After you change the configuration, you must save the changes to both the master and the standby CP modules. Save the configuration to a file to retain the configuration settings.

Before you begin

- You must log on to the Privileged EXEC mode in ACLI.
- To save a file to the standby CP module, you must enable the Trivial File Transfer Protocol (TFTP) on the standby CP module.

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.

Procedure

Save the running configuration:

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

Example

```
VSP-9012:1>enable
```

Save the configuration to the default location:

```
VSP-9012:1>save config
```

Identify the file as a backup file and designate a location to save the file:

```
VSP-9012:1#save config backup 4717:0:0:0:0:0:7933:6:/configs/
backup.cfg
```

Variable definitions

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

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following formats: • x:x:x:x:x:x:x:<file> • a.b.c.d:<file> • peer:<file> • /intflash/ <file> • /extflash/ <file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following formats: • x:x:x:x:x:x:x:<file> • a.b.c.d:<file> • peer:<file> • /intflash/ <file> • /extflash/ <file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
standby *WORD<1–99>*	Saves the specified file name to the standby CPU in the following formats:

Variable	Value
	• /intflash/ <file> • /extflash/ <file> • /usb/ <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. You cannot use this variable if you enable HA mode.

Backing up and restoring the compact flash to USB

Perform this procedure to back up and restore the contents of the internal or external 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 or want to replace the existing compact flash card or CP module without losing the data.

Before you begin

- You must log on to at least Privileged EXEC mode in ACLI.
- You must have a USB storage device ready to use. Avaya supports USB 1 and 2. The memory size must be at least 2 GB. Avaya recommends that you use an Avaya USB storage device. For more information, see *Avaya Virtual Services Platform 9000 Release Notes*, NN46250–401.

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` and `/usb/extflash/extflashbackup_yyyymmddhhmmss.tgz`.

Logging is automatically disabled on the compact flash during backup.

The backup action can take up to 10 minutes.

Procedure

1. Backup the internal flash to USB:
   ```
   backup intflash
   ```
2. Backup the external flash to USB:

```
backup extflash
```

3. Restore the data to the internal flash:
   ```
   restore intflash
   ```
4. Restore the data to the external flash:
   ```
   restore extflash
   ```
5. Ensure that logging is enabled for the external compact flash.

Example

```
VSP-9012:1#backup intflash

Warning: Internal flash is being used for logging right now.
       Backup/Restore intflash is not allowed. Please use the
       following CLI command in the global configuration mode
       to disable the logging to intflash, then try again.

 Case 1: If extflash is not present, disable the global logging.
       Command: no boot config flags logging

 Case 2: If extflash is present, enable logging to extflash.
       Command: logging logToExtFlash

 Execute  Command: logging logToExtFlash

 LoggingToPcmcia 1 LoggingToIntflash 0


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:
          1934917632 total bytes on the filesystem
           643297280 used bytes on the filesystem
          1291620352 free bytes on the filesystem

For file system /usb:
          3990487040 total bytes on the filesystem
           499318784 used bytes on the filesystem
          3491168256 free bytes on the filesystem

cd /intflash ; /bin/tar -czvf /usb/intflash/intflashbackup_20110420212218.tgz
* ; /bin/sync

Info: Backup /intflash to filename /usb/intflash/intflashbackup_20110420212218.tgz
is complete!

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

Logging to Intflash stopped

Logging to Extflash started
```

Restarting the platform

Before you begin

- You must log on to Privileged EXEC mode in ACLI.

Note:

The command mode is key 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 switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify the boot source (internal flash, external flash, USB, or TFTP server) and file name. If you do not specify a device and file, the run-time ACLI uses the software and 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 a restart. If a CPU (9080CP module) switchover occurs during operation, the switch sends a warm-start management trap within 45 seconds of a restart.

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

Procedure

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-9012:1>enable
```

Restart the switch:

```
VSP-9012:1#boot config /intflash/config.cfg
VSP-9012:1# Do you want to continue? (y/n)
```

```
VSP-9012:1# Do you want to continue? (y/n)y
```

Variable definitions

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

Table 1: Variable definitions

Variable	Value
config *WORD<1–99>*	Specifies the software configuration device and file name in one of the following formats: • a.b.c.d:<file> • /intflash/ <file> • /extflash/ <file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
-y	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the system restarts.

Resetting the platform

Before you begin

• You must log on to Privileged EXEC mode in ACLI.

About this task

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

Procedure

Reset the switch:

```
reset [-y]
```

Example

```
VSP-9012:1>enable
```

Reset the switch:

```
VSP-9012:1#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.

Accessing the standby CPU

Before you begin

- The Telnet daemon is activated.
- You must configure an rlogin access policy on the standby CPU before you can use the peer command to access it from the master CPU using rlogin. By default, the remote access services are disabled. To configure an access policy on the standby CPU, connect a terminal to the console port on the standby CPU. For more information about the access policy commands, see *Avaya Virtual Services Platform 9000 Commands Reference — ACLI*, NN46250–104.
- You must log on to Privileged EXEC mode in ACLI.

About this task

Access the standby CPU to make changes to the standby CPU without reconnecting to the console port on that module.

Procedure

Access the standby CPU:

```
peer {telnet|rlogin}
```

Example

```
VSP-9012:1>enable
```

Specify the access method to use to connect to the standby CPU to rlogin:

```
VSP-9012:1#peer rlogin
```

Variable definitions

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

Table 3: Variable definitions

Variable	Value
{telnet|rlogin}	Specifies the access method to use to connect to the standby CPU.

Pinging an IP device

Before you begin

- You must log on to User EXEC mode in ACLI.

About this task

Ping a device to test the connection between Avaya Virtual Services Platform 9000 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

Ping an IP network connection:

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

Example

Ping an IP device through the management interface:

```
VSP-9012:1>ping 192.0.2.16 vrf mgmtrouter

192.0.2.16 is alive
```

Variable definitions

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

Table 4: 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 <16–51200>	Specifies the size of ping data sent in bytes (16–51200). The default is 16.
interface WORD <1–256>	Configures a specific outgoing interface to use by IP address. Additional ping interface filters: • gigabitEthernet: {slot/port} gigabit ethernet port • mgmtEthernet: {slot/port} management ethernet port • tunnel: tunnel ID as a value from 1–2147477248 • vlan: VLAN ID as a value from 1–4094
-I <1–60>	Specifies the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the [-I] 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. Specify the MgmtRouter VRF if you need to run the ping operation through the management interface.

Variable	Value
WORD<0–256>	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x: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.
- You must log on to Privileged EXEC mode in ACLI.

About this task

Calculate the MD5 digest to verify the MD5 checksum. The **md5** command calculates the MD5 digest for files on the internal or external 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

Calculate the MD5 digest:

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

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

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

```
VSP-9012:1(config)#md5 password —a
```

Variable definitions

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

Table 5: 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 *WORD<1–99>* 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 `/intflash/checksum.md5` 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 <*filename*> not present. The -c option also • calculates the checksum of files specified by *WORD<1–99>* • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison

-f WORD<1–99>	Stores the result of MD5 checksum to a file on internal or external 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.`
	If the output file specified with the -f option is files for which to compute MD5 checksum, the command fails with the error message:
	`VSP-9012:1# md5 *.cfg -f config.cfg Error: Invalid operation on file <filename>`
	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:
	`File exists. Do you wish to overwrite? (y/n)`

Variable	Value
-r	Reverses the output. Use with the -f option to store the output to a file. You cannot use the -r option with the -c option.

Resetting system functions

Before you begin

- You must log on to Global Configuration mode of ACLI.

About this task

Reset system functions to reset all statistics counters, the console port, and the operation of the switchover function.

Procedure

1. Change to the backup CPU:
   ```
   sys action cpu-switch-over
   ```
2. Reset system functions:
   ```
   sys action reset {console|counters}
   ```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal
```

Reset the switch to change over to the backup CPU:

```
VSP-9012:1(config)# sys action cpu-switch-over
```

Reset the statistics counters:

```
VSP-9012:2(config)# 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 6: Variable definitions

Variable	Value
cpu-switch-over	Resets the switch to change over to the backup CPU.
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

Before you begin

- You must log on to Privileged EXEC mode in ACLI.

About this task

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

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

Warning:

You are not able to source a complete configuration file to merge it with your running configuration because the system can crash. The source command can be used to merge smaller portions of a configuration into the existing configuration.

Procedure

Source a configuration:

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

Example

```
VSP-9012:1>enable
```

Debug the script output:

```
VSP-9012:1#source 192.0.2.3 debug
```

Variable definitions

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

Table 7: 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: • x:x:x:x:x:x:x:x:<file> • a.b.c.d:<file> • peer:<file> • /intflash/ <file> • /extflash/ <file> • /usb/<file> <file> is a string. The path and <file> can use 1–99 characters.

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 9000 operations using Enterprise Device Manager (EDM).

Where mentioned, configuration files are ASCII text files that allow an administrator to change switch configuration quickly.

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. Select **Configuration** > **Edit** > **Chassis**.
2. Click the **System** tab.
3. Locate **ActionGroup4** near the bottom of the screen.
4. Select **softReset** from **ActionGroup4**.
5. Click **Apply**.

Showing the MTU for the system

About this task

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

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.

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

Displaying storage use

About this task

Display the amount of memory used and available for both onboard flash memory and installed external storage devices, as well as the number of files in each location.

Procedure

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

Device Info field descriptions

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

Name	Description
Slot	Specifies the slot number of the CP module.
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.
ExtflashBytesUsed	Specifies the number of bytes used in external flash memory.
ExtflashBytesFree	Specifies the number of bytes available for use in external flash memory.
ExtflashNumFiles	Specifies the number of files in external flash memory.
UsbBytesUsed	Specifies the number of bytes used on the USB device.
UsbBytesFree	Specifies the number of bytes available on the USB device.

Name	Description
UsbNumFiles	Specifies the number of files on the USB device.

Displaying flash file information

About this task

Display information about the files in internal flash memory for all CP modules to view general file information.

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

Displaying external flash file information

About this task

Display information about the files in external flash memory for all CP modules to view general file information.

Procedure

1. In the navigation tree, open the following folders:**Configuration** > **Edit**.

2. Click **File System**.
3. Click the **External Flash Files** tab.

External Flash Files field descriptions

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

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

About this task

Display information about the files on a USB device for all CP modules to view general file information.

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.

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.

Name	Description
Size	Specifies the size of the file.

Displaying available storage space

About this task

Display information about the available space for storage devices on a specific CP module.

Procedure

1. In the Device Physical View tab, select a CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Storage Usage** tab.

Storage Usage field descriptions

Use the data in the following table to use the **Storage Usage** 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.
ExtflashBytesUsed	Specifies the number of bytes used in external flash memory.
ExtflashBytesFree	Specifies the number of bytes available for use in external flash memory.
ExtflashNumFiles	Specifies the number of files in external flash memory.
UsbBytesUsed	Specifies the number of bytes used on the USB device.
UsbBytesFree	Specifies the number of bytes available on the USB device.
UsbNumFiles	Specifies the number of files on the USB device.

Displaying internal flash files for a CP module

About this task

Display information about the files on the internal flash for a specific CP module.

Procedure

1. In the Device Physical View tab, select a CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Flash Files** tab.

Flash Files field descriptions

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

Name	Description
Name	Specifies the directory name of the flash file.
Date	Specifies the creation or modification date of the flash file.
Size	Specifies the size of the flash file.

Copying a file

About this task

Copy files between the internal flash and external storage. The source and destination options are

- /intflash/
- /extflash/
- /usb/

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 cancels the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

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.

Name	Description
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.
VirtualIpAddr	Configures the virtual IP address that is advertised by the primary CPU and stored in the switch configuration file.
VirtualNetMask	Configures the net mask of the virtual management IP address.
VirtualIpv6Address	Configures the virtual IPv6 address that is advertised by the primary CPU. and stored in the switch configuration file.
VirtualIPv6Prefix Length	Configures the length of the virtual IPv6 prefix entry.
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.
LastRunTimeConfigSaveToSlave	Displays the last run-time configuration saved to the standby device.
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: • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration

Name	Description
	• saveRuntimeConfigToSlave—saves the current run-time configuration to the standby CPU • loadLicense—loads a software license file to enable features
ActionGroup2	Can be following action: • resetIstStatCounters—resets the IST statistic counters
ActionGroup3	Can be the following action: • flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be one of the following actions: • softReset—resets the device without running power-on tests • cpuSwitchOver—switch control from one CPU to another
Result	Displays a message after you click **Apply**.

Saving the configuration

About this task

After you change the configuration, you must save the changes to both the master and the standby CP modules. You can save configuration changes or changes to the boot parameters. 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 navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System** tab.
4. Optionally, specify a filename in **ConfigFileName**.

If you do not specify a filename, the system saves the information to the default file.

5. In **ActionGroup1**, select **saveRuntimeConfig**.
6. 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 9000. Review this content before you make changes to the configurable boot process options.

Boot sequence

The Virtual Services Platform 9000 goes through a three-stage boot sequence before it becomes fully operational. After you turn on power to the switch, the Control Processor (CP) module starts. In Virtual Services Platform 9000 with redundant CP modules, the module in slot 1 provides the active CPU functions after the system powers up or resets.

The boot sequence consists of the following stages:

- Stage 1: Loading Linux on page 40
- Stage 2: Loading the primary release on page 41
- Stage 3: Loading the configuration file on page 41

The following figure shows a summary of the boot sequence.

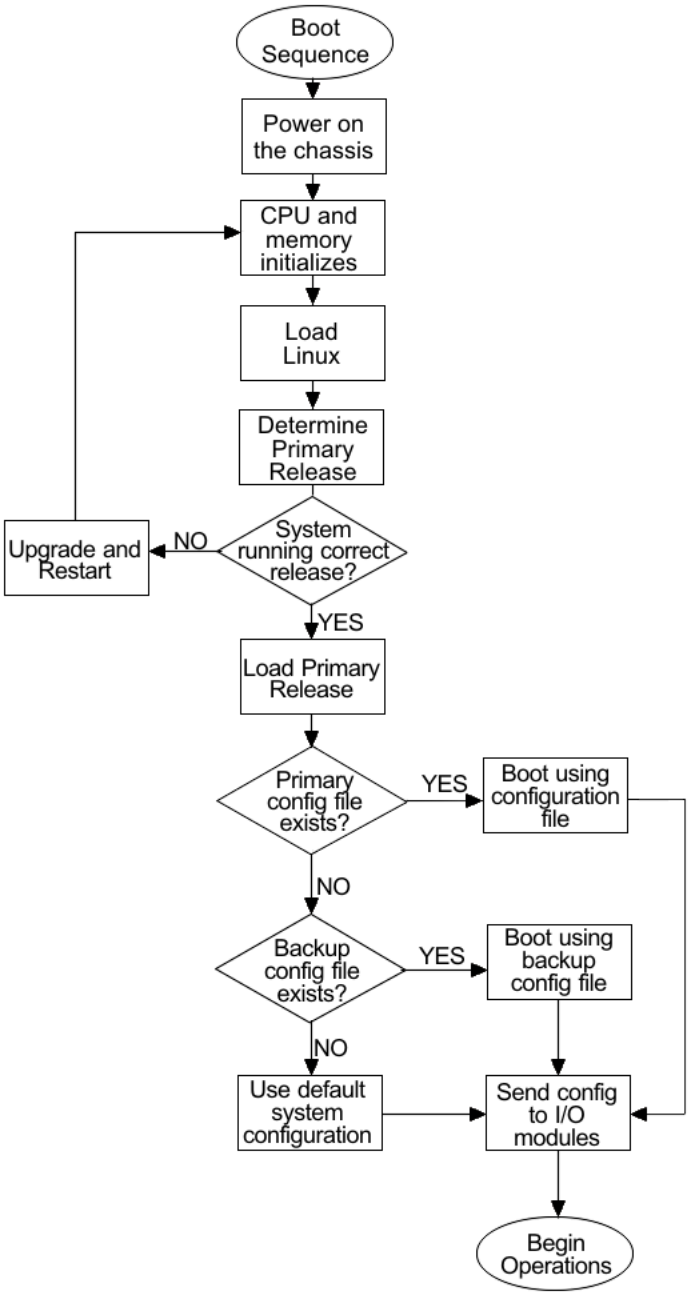

Figure 1: Virtual Services Platform 9000 boot sequence

Stage 1: Loading Linux

The CP, IO, and SF modules contain a boot flash that stores the boot images, which include the boot loader, and the Linux kernel and applications. The boot flash 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.

The boot process conducts a power-on-self-test (POST). The results of POST save to NVRAM. If the POST passes, the process continues and loads Linux on the CP, input/output (I/O), and Switch Fabric (SF) modules.

The I/O and SF modules wait for the master CP module to activate before they continue to stage 2.

Stage 2: Loading the primary release

After Linux starts, the system looks for version.cfg on the internal flash of the CP module. Virtual Services Platform 9000 can install a maximum of six releases but can only load one of two—a primary (committed) release or a backup release.

The system reads the primary release from version.cfg, and then confirms all modules use the correct release. If a module does not use the correct release, the system upgrades or downgrades the module, and then restarts the module. The system saves software image files to the /intflash/release/ directory.

If you insert a new module in a running system, the software and firmware automatically update to the primary release.

After loading the primary release, the CPU and basic system devices such as the console port and external storage slots initialize. At this stage, the I/O ports and the management port are not available; the system does not initialize the I/O ports and management port until the CP 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 store this file in internal flash, external flash, or on a USB device. The default location is the internal flash but you can modify this parameter in ACLI.

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 44.

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 8: Configuration file statements

Sample statement	Action
`# software version : 3.0.0.0`	Adds clarity to the configuration by identifying the software version.
`#!no boot config flags sshd`	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 after you 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.

Run-time

After Virtual Services Platform 9000 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 9000
- 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.

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 54.

Table 9: Boot config flags

ACLI flag	Restart
`block-snmp`	No
`debug-config`	Yes
`debugmode`	Yes
`fabric-profile`	Yes
`factorydefaults`	Yes
`ftpd`	No
`ha-cpu`	Yes, the standby CPU restarts automatically. Modifying this flag does not require a system restart.
`hsecure`	Yes
`logging`	No
`reboot`	Yes
`rlogind`	No
`savetostandby`	No
`spanning-tree-mode`	Yes
`sshd`	No

ACLI flag	Restart
telnetd	No
tftpd	No
trace-logging	No
verify-config	Yes
wdt	Yes

System connections

Connect the serial console interface (an RS-232 port) to a PC or terminal to monitor and configure the switch. The port uses a DB-9 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 the following equipment:

- a terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software
- an Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the switch. The other end of the cable must use a connector appropriate to the serial port on your computer or terminal. You can find a null modem cable with the chassis.

You must shield the cable that connects to the console port to comply with emissions regulations and requirements.

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 9000 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:

Virtual Services Platform 9000 supports the following active ACLI clients using IPv4:

- remote shell (rsh)
- rlogin
- Secure Shell (SSH)

Virtual Services Platform 9000 supports the following non active client using IPv4:

- Network Time Protocol (NTP)

IPv4 and IPv6 support:

Virtual Services Platform 9000 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 9000 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:

Virtual Services Platform 9000 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 Shell (SSH)
- 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 *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

Modifying the boot sequence

Before you begin

- You must log on to Global Configuration mode in ACLI.

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. Bypass the loading of the switch configuration file and load the factory defaults:
   ```
   boot config flags factorydefaults
   ```
2. 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, ensure you use the no operator with this command, **`no boot config flags factorydefaults`**, before you investigate other options.

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#boot config flags factorydefaults
```

Configuring the remote host logon

Before you begin

- You must enable Global Configuration mode in ACLI.
- 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. 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>}
   ```

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

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Enable console tftp/tftpd debug messages:

```
VSP-9012:1(config)#boot config host tftp-debug

VSP-9012:1(config)#save config

VSP-9012:1(config)#reset
```

Enabling remote access services

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 *Avaya Virtual Services Platform 9000 Security*, NN46250–601.
- You must log on to Global Configuration mode in ACLI.

About this task

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

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

On IPv6 networks, VSP 9000 supports SSH server and Remote Shell (rsh) server only. VSP 9000 does not support outbound SSH client over IPv6 or rsh client over IPv6. On IPv4 networks, VSP 9000 supports both server and client for SSH and rsh.

Procedure

1. Enable the access service:
   ```
   boot config flags {ftpd|rlogind|sshd|telnetd|tftpd}
   ```
2. Save the configuration.

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Specifiy the Rapid Spanning Tree Protocol Mode. The default is MSTP:

```
VSP-9012:1(config)#boot config flags spanning-tree—mode rstp
```

Variable definitions

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

Table 10: 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 [file]	Activates or disables run-time debugging of the configuration file. If you activate debugging, line-by-line configuration file processing appears on the console during CPU initialization. The default value is disabled. File logs the debug-config output to /extflash/debugconfig.txt If you change the debug-config variable value, you must restart the switch.
debugmode	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the **`trace`** commands. If you enable this flag, the switch does not restart following a fatal error. The default value is disabled. If you change this parameter, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
fabric-profile <1–3>	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are • 1: balanced • 2: unicast optimized • 3: multicast optimized If you change this parameter, you must restart the switch. The default profile is 1, balanced.
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

Variable	Value
	enable FTP, ensure that the tftpd flag is disabled.
ha-cpu	Activates or disables High Availability (HA) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable or disable High Availability mode, the secondary CPU resets automatically to load settings from the saved configuration file.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • aging time • failed login attempt limitation 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.
logging	The logging command is used to activate or disable system logging. The default value is enabled. The system names log files according to the following: • File names appear in 8.3 (log.xxxxxxxx.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. The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated. The reboot command is equivalent to the

Variable	Value
	debugmode command. If you change the reboot variable value, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby	Activates or disables automatic save of the configuration file to the standby CPU. The default value is enabled. If you operate a dual CPU system, Avaya recommends that you enable this flag for ease of operation.
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.
sshd	Activates or disables the SSH server service. The default value is enabled.
telnetd	Activates or disables the Telnet server service. The default is disabled. If you disable the Telnet server service in a dual CPU system, the Telnet server prevents a Telnet connection initiated from the other CPU.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled. If you disable the TFTP server you can still copy files between the CPUs.
trace-logging	Activates or disables the creation of trace logs. The default value is disabled. **Important:** Do not change this parameter unless directed by Avaya.
verify-config	Activates syntax checking of the configuration file. The default value is enabled. If the system finds a syntax error, it loads the factory default configuration. If you disable this flag, the system logs syntax

Variable	Value
	errors and the CPU continues to source the configuration file. Avaya recommends that you disable the verify-config flag. If you change this parameter, you must restart the switch.
wdt	Activates or disables the hardware watchdog timer monitoring a hardware circuit. The default value is activated. The watchdog timer restarts the switch based on software errors. If you change the wdt flag, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.

Changing the boot source order

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Change the boot source order to specify which configuration file the system uses to start. Configure the primary boot choices.

By default, the primary source is the internal flash. If you change the primary source, the system uses the location you specify. If no configuration file exists in the location you specify, the system accesses the default locations. If the default locations do not contain a configuration or backup configuration file, the system loads the default configuration.

Procedure

1. Change the primary boot choice:
   ```
   boot config choice primary {backup-config-file|config-file}
   WORD<0-255>
   ```
2. Save the changed configuration.
3. Restart the switch.

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

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

```
VSP-9012:1(config)# boot config choice primary config-file /extflash/
config.cfg
VSP-9012:1(config)# save config
VSP-9012:1(config)# reset
```

Variable definitions

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

Table 11: 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. *WORD<0–255>* is the device and file name, up to 255 characters including the path, in one of the following formats: • x:x:x:x:x:x:x:x:<file> • a.b.c.d:<file> • /intflash/<file> • /extflash/<file> • /usb/<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.
- You must log on to Global Configuration mode in ACLI.

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 both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

On IPv6 networks, VSP 9000 supports SSH server, remote login (rlogin) server and Remote Shell (rsh) server only. VSP 9000 does not support outbound SSH client over IPv6, rlogin client over IPv6 or rsh client over IPv6. On IPv4 networks, VSP 9000 supports both server and client for SSH, rlogin and rsh.

Procedure

1. Enable system flags:

   ```
   boot config flags <block-snmp|debug-config [file]|debugmode|
   fabric-profile <1-3>|factorydefaults|ftpd|ha-cpu|hsecure|
   logging|reboot|rlogind|savetostandby|spanning-tree-
   mode <mstp|rstp>|sshd|telnetd|tftpd|trace-logging|verify-
   config|wdt>
   ```

2. Disable system flags:

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

3. Configure the system flag to the default value:

   ```
   default boot config flags <block-snmp|debug-config [file]|
   debugmode|fabric-profile|factorydefaults|ftpd|ha-cpu|
   hsecure|logging|reboot|rlogind|savetostandby|spanning-tree-
   mode|sshd|telnetd|tftpd|trace-logging|verify-config|wdt>
   ```

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

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Activate High Secure mode:

```
VSP-9012:1(config)#boot config flags hsecure

VSP-9012:1(config)#save config
```

```
VSP-9012:1(config)#reset
```

Variable definitions

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

Table 12: 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 [file]	Activates or disables run-time debugging of the configuration file. If you activate debugging, line-by-line configuration file processing appears on the console during CPU initialization. The default value is disabled. File logs the debug-config output to /extflash/debugconfig.txt If you change the debug-config variable value, you must restart the switch.
debugmode	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the **`trace`** commands. If you enable this flag, the switch does not restart following a fatal error. The default value is disabled. If you change this parameter, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
fabric-profile <1–3>	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are • 1: balanced • 2: unicast optimized • 3: multicast optimized If you change this parameter, you must restart the switch. The default profile is 1, balanced.

Variable	Value
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.
ha-cpu	Activates or disables High Availability (HA) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable or disable High Availability mode, the secondary CPU resets automatically to load settings from the saved configuration file.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • aging time • failed login attempt limitation 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.
logging	The logging command is used to activate or disable system logging. The default value is enabled. The system names log files according to the following: • File names appear in 8.3 (log.xxxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address.

Variable	Value
	• 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. The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated. The reboot command is equivalent to the debugmode command. If you change the reboot variable value, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby	Activates or disables automatic save of the configuration file to the standby CPU. The default value is enabled. If you operate a dual CPU system, Avaya recommends that you enable this flag for ease of operation.
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.
sshd	Activates or disables the SSH server service. The default value is enabled.
telnetd	Activates or disables the Telnet server service. The default is disabled. If you disable the Telnet server service in a dual CPU system, the Telnet server prevents a Telnet connection initiated from the other CPU.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is

Variable	Value
	disabled. If you disable the TFTP server you can still copy files between the CPUs.
trace-logging	Activates or disables the creation of trace logs. The default value is disabled. **Important:** Do not change this parameter unless directed by Avaya.
verify-config	Activates syntax checking of the configuration file. The default value is enabled. If the system finds a syntax error, it loads the factory default configuration. If you disable this flag, the system logs syntax errors and the CPU continues to source the configuration file. Avaya recommends that you disable the verify-config flag. If you change this parameter, you must restart the switch.
wdt	Activates or disables the hardware watchdog timer monitoring a hardware circuit. The default value is activated. The watchdog timer restarts the switch based on software errors. If you change the wdt flag, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.

Specifying the master CPU and the standby-to-master delay

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Specify the master CPU to designate which CPU becomes the master after the switch performs a full power cycle.

Configure the standby-to-master delay to set the number of seconds a standby CPU waits before trying to become the master CPU. The standby-to-master delay applies when two CP modules are booting at the same time. The designated standby CP waits for the configured

number of seconds before attempting to assert mastership. Only one CP can be master in a chassis.

Warning:

Configuring this to too short a value can result in the configured standby CP becoming a master. Configuring it too long can delay the backup CP asserting mastership and continue booting when the designated CP is inserted, but fails booting.

Procedure

1. View the current configuration for the master CPU:
   ```
   show boot config master
   ```
2. Specify the slot of the master CPU:
   ```
   boot config master <1-2>
   ```
3. Save the changed configuration.
4. Configure the number of seconds a standby CPU waits before trying to become the master CPU:
   ```
   boot config delay <0-255>
   ```
5. Save the changed configuration.
6. Restart the switch.

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Specify the slot number, either 1 or 2, for the master CPU:

```
VSP-9012:1(config)#boot config master 2
VSP-9012:1(config)#save config
```

Specify the number of seconds a standby CPU waits before trying to become the master CPU:

```
VSP-9012:1(config)#boot config delay 30
VSP-9012:1(config)#save config
VSP-9012:1(config)#reset
```

Variable definitions

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

Table 13: Variable definitions

Variable	Value
<1–2>	Specifies the slot number, either 1 or 2, for the master CPU. The default value is slot 1.

Configuring the CP module network port

Before you begin

- You must log on to mgmtEthernet Interface Configuration mode in ACLI.

About this task

Configure the network port devices to define connection settings for the Ethernet management (mgmt) port. The steps in this procedure are optional. You can use the default configuration.

Procedure

1. Activate auto-negotiation for the port:
   `auto-negotiate enable`
2. If you do not use auto-negotiation, configure the duplex mode:
   `duplex <half|full>`
3. Assign an IPv4 address to the port:
   `ip address {A.B.C.D A.B.C.D|A.B.C.D/X}`
4. Assign an IPv6 address to the port:
   `ipv6 interface address WORD<0-255>`
5. Disable the port:
   `shutdown`

   To restart the port, use `no shutdown` to enable it again.
6. Configure the speed for the port:
   `speed <10|100>`
7. Save the changed configuration.

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface mgmtEthernet 2/1
```

Activate auto-negotiation for the port:

```
VSP-9012:1(config-if)#auto-negotiate enable
```

If you do not use auto-negotiation, specify full-duplex mode:

```
VSP-9012:1(config-if)#duplex full
```

Assign an IPv4 address and mask for the management port:

```
VSP-9012:1(config-if)#ip address 192.0.2.40/255.255.255.0
```

Assign an IPv6 address to the management port:

```
VSP-9012:1(config-if)#ipv6 interface address 2001:100:102:202::1
```

Disable the port:

```
VSP-9012:1(config-if)#shutdown
```

Restart the port:

```
VSP-9012:1(config-if)#no shutdown
```

Configure the connection speed for ports to 100 Mb/s:

```
VSP-9012:1(config-if)#speed 100
```

Save the changed configuration:

```
VSP-9012:1(config-if)#save config
```

Variable definitions

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

Table 14: Variable definitions

Variable	Value
<half|full>	Specifies half- or full-duplex mode. The default value is half. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Use the data in the following table to use the `ip address` and `ipv6 interface address` commands.

Table 15: Variable definitions

Variable	Value
{A.B.C.D A.B.C.D|A.B.C.D/X}	Assigns an IP address and mask for the management port.

Variable	Value
	Important: You cannot assign an address of 0.0.0.0/0.
ipv6 interface address*WORD<0–255>*	Assigns an IPv6 address to the management port.

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

Table 16: Variable definitions

Variable	Value
speed <10|100>	Configures the connection speed for ports to 10 Mb/s or 100 Mb/s. The default is 10 Mb/s. To configure this option to the default value, use the default operator with the command.

Assigning an IP address to the management port

Before you begin

- You must log on through the CP console, enter Global Configuration mode, and then navigate to `interface mgmtEthernet [1/1|2/1]` in ACLI.

About this task

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Procedure

1. Assign an IP address to the management port:
   `ip address {A.B.C.D} {A.B.C.D}`
2. Exit to Global Configuration mode.
3. Assign an IPv4 address to a virtual management port:
   `sys mgmt-virtual-ip {A.B.C.D/X}`
4. Assign an IPv6 address to a virtual management port:
   `ipv6 mgmt-virtual WORD<0-46>`

5. Save the configuration.

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
VSP-9012:1(config)# interface mgmtEthernet 1/1
VSP-9012:1(config-if)# sys mgmt-virtual-ip 192.0.2.40/255.255.255.0
VSP-9012:1(config-if)# exit
VSP-9012:1(config)# sys mgmt-virtual-ip 192.0.2.60/255.255.255.0
VSP-9012:1(config)# save config
The physical and virtual IP must be in the same subnet.
```

Variable definitions

Use the data in the following table to use the `ip address` command.

Table 17: Variable definitions

Variable	Value
{A.B.C.D} {A.B.C.D}	Specifies the IP address and subnet mask for the management port on the CP module. **Important:** You cannot assign an address of 0.0.0.0/0.

Use the data in the following table to use the `sys mgmt-virtual-ip` command.

Table 18: Variable definitions

Variable	Value
{A.B.C.D/X}	Specifies the IP address and subnet mask in the format A.B.C.D/x or A.B.C.D/x.x.x.x. (for example, 192.0.2.15/255.255.255.0). **Important:** You cannot assign an address of 0.0.0.0/0.

Use the data in the following table to use the `ipv6 mgmt-virtual` command.

Table 19: Variable definitions

Variable	Value
WORD<0–46>	Specifies the IPv6 address in hexadecimal format (string length 0–46) and the prefix-length.

Configuring CP module serial port devices

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

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

Procedure

1. Optionally, specify 8 data bits:
   `boot config sio console 8databits`
2. Optionally, change the baud rate for the port:
   `boot config sio console baud <9600–115200>`
3. Save the changed configuration.
4. Restart the switch.

Example

```
VSP-9012:1>enable
VSP-9012:1#config terminal
```

Configure the baud rate to 9600 for the port:

```
VSP-9012:1(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 20: 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 no 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: • 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 monitor configuration

Before you begin

- You must log on to Privileged EXEC mode in ACLI.

About this task

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

Procedure

View the configuration:

```
show boot config <choice|flags|general|host|master|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-9012:1>enable
VSP-9012:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSP-9012:1(config)#show boot config running-config
#
# Thu Jun 30 15:12:01 2011 UTC
#
boot config flags fabric-profile 1
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 21: 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.
master	Identifies the current CP module slot configured as master and shows the current master 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 CP module 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 *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

Configuring the date

Before you begin

- You must log on to Privileged EXEC mode in ACLI.
- 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

Configure the date:

```
clock set <MMddyyyyhhmmss>
```

Example

```
VSP-9012:1>enable
VSP-9012:1#clock set 11062011063030
```

Variable definitions

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

Table 22: Variable definitions

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

Configuring the time zone

Before you begin

- You must log on to Global Configuration mode in ACLI.

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 from 1901 to 2038. You do not need to configure daylight savings.

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

Procedure

1. Configure the time zone by using the following command:
   `clock time-zone WORD<1–10> WORD<1–20> WORD<1–20>`
2. Save the changed configuration.

Example

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

```
VSP-9012:1(config)#clock time-zone America Indiana Vevay
```

Variable definitions

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

Table 23: Variable definitions

Variable	Value
WORD<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 `clock time-zone`

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

Configuring the run-time environment

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

Procedure

1. Change the login prompt:
   `login-message` *`WORD<1-1513>`*
2. Change the password prompt:
   `passwordprompt` *`WORD<1-1510>`*
3. Configure the number of supported rlogin sessions:
   `max-logins` *`<0-8>`*
4. Configure the number of supported inbound Telnet sessions:
   `telnet-access sessions` *`<0-8>`*
5. Configure the idle timeout period before automatic logoff for ACLI and Telnet sessions:
   `cli timeout` *`<30-65535>`*
6. Configure the number of lines in the output display:
   `terminal length` *`<8-64>`*
7. Configure scrolling for the output display:

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

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

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

```
VSP-9012:1(config)#default login-message
```

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

```
VSP-9012:1(config)#default passwordprompt
```

Configure the allowable number of inbound remote ACLI logon sessions:

```
VSP-9012:1(config)#max-logins 5
```

Configure the allowable number of inbound Telnet sessions:

```
VSP-9012:1(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-9012:1(config)#cli timeout 900
```

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

```
VSP-9012:1(config)#terminal length 30
```

Configure scrolling for the output display:

```
VSP-9012:1(config)#terminal more disable
```

Variable definitions

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

Table 24: Variable definitions

Variable	Value
WORD<1-1513>	Changes the ACLI logon prompt. • *WORD<1-1513>* is an American Standard Code for Information Interchange (ASCII) string from 1–1513 characters. • Use the default option before this parameter, `default login-message`, to enable use of the default logon string. • Use the no operator before this parameter, `no login-message`, to disable the default logon banner and display the new banner.

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

Table 25: Variable definitions

Variable	Value
WORD<1-1510>	Changes the ACLI password prompt. • *WORD<1-1510>* is an ASCII string from 1–1510 characters. • Use the default option before this parameter, `default passwordprompt`, to enable using the default string. • Use the no operator before this parameter, `no passwordprompt`, to disable the default string.

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

Table 26: 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 27: 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 28: 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 29: 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 thedefault operator with the command. The default is value 23.
disable|enable	Configures scrolling for the output display. The default is enabled. Use the no 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

Procedure

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

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

2. Create a custom banner:

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

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Activate the use of the default banner:

```
VSP-9012:1(config)#banner static
```

Variable definitions

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

Table 30: Variable definitions

Variable	Value
custom|static	Activates or disables use of the default banner.
WORD<1–80>	Adds lines of text to the ACLI logon banner.

Configuring the message-of-the-day

Before you begin

- You must log on to Global Configuration mode in ACLI.

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. Create the message-of-the-day:

```
banner motd WORD<1-1516>
```

2. Enable the custom message-of-the-day:

```
banner displaymotd
```

Example

```
VSP-9012:1>enable

VSP-9012:1#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-9012:1(config)#banner motd "Unauthorized access is forbidden"
```

Enable the custom message-of-the-day:

```
VSP-9012:1(config)#banner displaymotd
```

Variable definitions

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

Table 31: Variable definitions

Variable	Value
WORD<1–1516>	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

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

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.

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. Enable ACLI logging:
   ```
   clilog enable
   ```
2. Disable ACLI logging:
   ```
   no clilog enable
   ```
3. Ensure that the configuration is correct:
   ```
   show clilog
   ```
4. View the ACLI log:
   ```
   show logging file module clilog
   ```
5. View the ACLI log. The following command only applies to log files generated by releases prior to Release 3.2:
   ```
   show clilog file [grep WORD<1-256>] [tail]
   ```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#clilog enable
```

```
VSP-9012:1(config)#show logging file module clilog
CP1  [08/21/11 14:29:57.231] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     1 CONSOLE rwa en
CP1  [08/21/11 14:29:58.771] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     2 CONSOLE rwa config t
CP1  [08/21/11 14:30:06.743] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     3 CONSOLE rwa source basic.cfg
CP1  [08/21/11 14:30:07.018] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     4 CONSOLE rwa config terminal
CP1  [08/21/11 14:30:07.026] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     5 CONSOLE rwa boot config flags fabric-profile 1
CP1  [08/21/11 14:30:07.027] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     6 CONSOLE rwa boot config flags ftpd
CP1  [08/21/11 14:30:07.028] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     7 CONSOLE rwa boot config flags rlogind
CP1  [08/21/11 14:30:07.029] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     8 CONSOLE rwa boot config flags sshd
CP1  [08/21/11 14:30:07.030] 0x002c0600 00000000 GlobalRouter CLILOG
INFO     9 CONSOLE rwa boot config flags telnetd
CP1  [08/21/11 14:30:07.031] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    10 CONSOLE rwa cli timeout 65535
CP1  [08/21/11 14:30:07.032] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    11 CONSOLE rwa password password-history 3
CP1  [08/21/11 14:30:07.033] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    12 CONSOLE rwa clilog enable
CP1  [08/21/11 14:30:07.034] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    13 CONSOLE rwa snmplog enable
CP1  [08/21/11 14:30:07.046] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    15 CONSOLE rwa interface mgmtEthernet 1/1
CP1  [08/21/11 14:30:07.047] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    16 CONSOLE rwa ip address 192.0.2.49 255.255.255.0
CP1  [08/21/11 14:30:07.049] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    17 CONSOLE rwa exit
```

```
CP1  [08/21/11 14:30:07.050] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    18 CONSOLE rwa interface GigabitEthernet 10/11
CP1  [08/21/11 14:30:07.051] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    19 CONSOLE rwa no shutdown
CP1  [08/21/11 14:30:07.053] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    20 CONSOLE rwa exit
CP1  [08/21/11 14:30:07.054] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    21 CONSOLE rwa interface gigabitethernet 10/11
CP1  [08/21/11 14:30:07.056] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    22 CONSOLE rwa ipv6 interface vlan 3
CP1  [08/21/11 14:30:07.079] 0x002c0600 00000000 GlobalRouter CLILOG
INFO    23 CONSOLE rwa ipv6 interface enable
```

Variable definitions

Use the data in the following table to use the **clilog** commands.

Table 32: Variable definitions

Variable	Value
enable	Activates ACLI logging. To disable, use the `no clilog enable` command.

Use the data in the following table to use the **show clilog file** command.

Note:

The **show clilog file** command only applies to log files generated by releases prior to Release 3.2.

Table 33: Variable definitions

Variable	Value
tail	Shows the last results first.
grep WORD<1-256>	Performs a string search in the log file. *WORD<1-256>* is the string, of up to 256 characters in length, to match.

Configuring system parameters

Before you begin

- You must log on to Global Configuration mode in ACLI.
- You must acquire and configure a virtual management IP address before you can enable virtual IP as the UDP source.

About this task

Configure individual system-level switch parameters to configure global options for Avaya Virtual Services Platform 9000.

Procedure

1. Change the system name:
   `sys name WORD<0-255>`
2. Enable support for Jumbo frames:
   `sys mtu 1950`
   OR
   `sys mtu 9600`
3. Enable the User Datagram Protocol (UDP) checksum calculation:
   `udp checksum`
4. Enable virtual IP as the UDP source:
   `udpsrc-by-vip`

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

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

```
VSP-9012:1(config)#sys name Floor3Lab2
```

Variable definitions

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

Table 34: Variable definitions

Variable	Value
mtu <*1950*|*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 *WORD<0–255>*	Configures the system, or root level, prompt name for the switch. *WORD<0–255>* is an ASCII string from 0–255 characters (for example, LabSC7 or Closet4).

Creating a virtual management port

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Create a virtual management port in addition to the physical management ports on the switch management modules.

After you assign an IP address to the virtual management port, the IP address provides access to both switch management modules. The master management module replies to all management requests sent to the virtual IP address, as well as to requests sent to its management port IP address. If the master management module fails and the standby management module takes over, the virtual management port IP address continues to provide management access to the switch.

Procedure

Create a virtual management port:

```
sys mgmt-virtual-ip <A.B.C.D/X|A.B.C.D A.B.C.D>
```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# sys mgmt-virtual-ip 192.0.2.40/255.255.255.0

Physical and Virtual IP must be in the same subnet
```

Variable definitions

Use the data in the following table to use the `sys mgmt-virtual-ip` command.

Table 35: Variable definitions

Variable	Value
A.B.C.D/X|A.B.C.D A.B.C.D	Specifies the IP address and mask in one of the following formats:

Variable	Value
	• A.B.C.D/x • A.B.C.D/x.x.x.x • A.B.C.D x.x.x.x

Configuring system message control

Before you begin

- You must log on to Global Configuration mode in ACLI.

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. Configure system message control action:
   ```
   sys msg-control action <both|send-trap|suppress-msg>
   ```
2. Configure the maximum number of messages:
   ```
   sys msg-control max-msg-num <2-500>
   ```
3. Configure the interval:
   ```
   sys msg-control control-interval <1-30>
   ```
4. Enable message control:
   ```
   sys msg-control
   ```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

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

```
VSP-9012:1(config)#sys msg-control action both
```

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

```
VSP-9012:1(config)#sys msg-control max-msg-num 2
```

Configure the message control interval in minutes:

```
VSP-9012:1(config)#sys msg-control control-interval 3
```

Enable message control:

```
VSP-9012:1(config)#sys msg-control
```

Variable definitions

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

Table 36: 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

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

Configure the force message control option:

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

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

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

```
VSP-9012:1(config)#sys force-msg ****
```

Variable definitions

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

Table 37: Variable definitions

Variable	Value
WORD<4-4>	Adds a forced message control pattern, where *WORD<4-4>* 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.

High Availability-CPU mode

Platforms with two CPUs use High Availability (HA)-CPU mode to recover quickly from a failure of the master CPU. You can configure the CPUs to operate in either HA mode or non-HA mode.

The default mode is HA enabled. To disable CPU-HA mode, use the **`no boot config flags ha-cpu`** command. To activate CPU-HA mode, use the **`boot config flags ha-cpu`** command.

If you want to switch from one mode to the other, the standby CP reboots automatically once you enable or disable the new mode. The master CP does not require rebooting. If you switch from one mode to the other, the standby CP restarts in the specified HA mode (hot standby) or Non-HA mode (warm standby). All other modules are not affected.

A limited number of protocols support only partial High Availability implementation when in HA-mode.

High Availability mode

In High Availability (HA) mode, also called hot standby, the platform synchronizes the two CPUs. The CPUs use the same configuration and forwarding tables.

In full HA implementation, both the configuration and runtime application data tables exist on the master CPU and the secondary CPU. The master CPU automatically updates the forwarding tables of the secondary CPU in real time.

If the master CPU fails, the secondary CPU takes over the master responsibility quickly and you do not see an impact on your network. If the master CPU fails, the I/O and SF modules continue to run, all full HA applications continue to run and full HA applications run consistency checks to verify the tables.

The following applications support full High Availability mode:

- Layer 1
  - Port configuration parameters
- Layer 2
  - Multiple Spanning Tree parameters
  - Quality of Service (QoS) parameters
  - Rapid Spanning Tree parameters
  - Shortest Path Bridging MAC (SPBM)
  - SMLT parameters
  - VLAN parameters
- Layer 3
  - ARP entries
  - Internet Group Management Protocol (IGMP) Snooping
  - IP Filters
  - Layer 3 Filters: access control entries, access control lists
  - Open Shortest Path First (OSPF)
  - Packet Capture (PCAP) tool
  - Prefix lists and route policies
  - Router Discovery
  - Routing Information Protocol (RIP)
  - Routed Split Multi-Link Trunking (RSMLT)
  - RSMLT edge support
  - Shortest Path Bridging MAC (SPBM)
  - Static and default routes
  - Virtual IP (VLANS)
  - Virtual Router Redundancy Protocol (VRRP)
  - VRF Lite
- Transport layer:
  - Network Load Balancing (NLB)
  - Remote Access Dial-In User Services (RADIUS)
  - UDP forwarding

Partial HA

A few applications in HA-mode have partial HA implementation. This means that the system synchronizes user configuration data (including interfaces, IPv6 addresses and static routes) between the master CPU and standby CPU.

However, for applications in HA-mode with partial HA implementation, the platform does not synchronize dynamic data learned by protocols. As a result, after failure those applications

need to restart and rebuild their tables. This operation causes an interruption to traffic that is dependent on a protocol or application with Partial HA support.

The following applications support Partial High Availability:

- Layer 3
  - Border Gateway Protocol (BGP)
  - Dynamic Host Configuration Protocol (DHCP) Relay
  - Internet Group Management Protocol (IGMP)
  - IPv6
  - Protocol Independent Multicast-Sparse Mode (PIM-SM)
  - Protocol Independent Multicast-Source Specific Mode (PIM-SSM)
- Application
  - VSP Talk

Non-High Availability mode

In non-HA mode, also called warm standby, the platform synchronizes the configuration setting between the master CPU and the standby CPU; however, the platform does not synchronize the running operation status.

In this state, when one of the failover scenarios happens, the standby CPU starts the VSP operational image, the I/O and Switch Fabric modules do a soft restart and reload the configuration. It is basically a faster reboot/reset of the system.

If the master CPU fails, the secondary CPU must restart the protocols before it can take on the master responsibility. VSP 9000 resets the I/O and SF modules and the CPU must also relearn the forwarding table information. These operations cause an interruption to traffic.

Hardware and software compatibility

The following tables describe the hardware and the minimum Avaya Virtual Services Platform 9000 software version required to support the hardware.

Table 38: Hardware and minimum software version

Chassis, switching fabrics, and control processors			Minimum software version	Part number
	9012VSP chassis	12-slot chassis	3.0	EC1402001-E6
	9090SF	Switch Fabric module	3.0	EC1404006-E6
	9080CP	Control Processor module	3.0	EC1404007-E6

Chassis, switching fabrics, and control processors			Minimum software version	Part number
Power Supplies				
	9006AC	1200–2000W AC Power Supply	3.0	EC1405A01-E6
Cooling modules				
	9012FC	Side Fan Tray	3.0	EC1411001-E6
	9012RC	Fabric Fan Tray	3.0	EC1411002-E6
Ethernet modules				
	9024XL	24-port 10GBASE-X SFP +/SFP	3.0	EC1404001-E6
	9048GB	48-port 1000BASE-X SFP	3.0	EC1404002-E6
	9048GT	48-port 10/100/1000BASE-T	3.0	EC1404003-E6
Compatible SFPs and SFP+s For more information about SFP and SFP+, see *Avaya Virtual Services Platform 9000 Installation — SFP Hardware Components*, NN46250–305				
	100BASE-FX SFP	1310 nm, 100 Mb/s Ethernet, multimode fiber, duplex LC connector	3.0	AA1419074-E6
	1000BASE-T SFP	Gigabit Ethernet, RJ-45 connector	3.0	AA1419043-E6
	1000BASE-SX DDI SFP	850 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419048-E6
	1000BASE-LX DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419049-E6
	1000BASE-XD DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419050-E6
		1550 nm, Gigabit Ethernet, duplex LC connector		AA1419051-E6
	1000BASE-ZX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419052-E6
	1000BASE-BX DDI SFP	1310 nm (tx) and 1490 nm (rx), 1490 nm (tx) 1310 nm (rx), Gigabit Ethernet, single-fiber LC connector	3.0	AA1419069-E6 (10 km at 1310 nm) AA1419076-E6 (40 km at 1310 nm) AA1419070-E6 (10 km at 1490 nm)

Chassis, switching fabrics, and control processors			Minimum software version	Part number
				AA1419077-E6 (40 km at 1490 nm)
	1000BASE-EX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419071-E6
	1000BASE DDI CWDM 40 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419053-E6 to AA1419060-E6.
	1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419061-E6 to AA1419068-E6.
	10GBASE-SR/SW SFP+	400m, 850nm MMF	3.0	AA1403015-E6
	10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF	3.0	AA1403017-E6
	10GBASE-LR/LW SFP+	10km, 1310nm SMF	3.0	AA1403011-E6
	10GBASE-ER/EW SFP+	40km, 1550nm SMF	3.0	AA1403013-E6
	10GBASE-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports	3.0	AA1403018-E6 to AA1403021-E6

Power management

Power management identifies the available power in the chassis, called the power budget, and determines if enough power is available to operate the installed components.

If the power usage exceeds the power budget, the system powers off the module with the lowest priority. After a power over-usage occurs, the system uses a Simple Network Management Protocol (SNMP) trap to send a message to the network administrator configured to receive the trap.

The system compares the total chassis power consumed against the total chassis power available, and verifies that if one power supply fails, enough power still remains to operate the chassis and components. If enough power is available to keep all modules powered on in the case of a single failed power supply, then the system is considered to have redundant power.

Note:

In a redundant power supply configuration, that is, a +1 configuration where the system has one or more power supplies above the actual requirement, the power management logic automatically employs load-sharing across all active power supplies. This load-sharing ensures that the switch draws power equally from all available power supplies to support the system requirements in a fully active model.

If the system does not have redundant power, then the system sends an SNMP trap to the receiver and a message to ACLI to inform you that the device no longer operates in redundant power mode.

Software lock-up detection

The software lock-up detect feature monitors processes on the master 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 limits. After the feature encounters an issue that can potentially lock up the master CPU, the master ends the process and restarts. In redundant CP configurations, the standby CPU takes over from the master.

The CPU logs details about suspended tasks in the log file. For additional information about log files, see *Avaya Virtual Services Platform 9000 Fault Management*, NN46250–703.

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 9000 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 *Avaya Virtual Services Platform 9000 Configuration — VLANs and Spanning Tree*, NN46250–500.

Modules and interfaces that support Jumbo frames

As a minimum, Jumbo frame support requires Gigabit speed.

The following devices and interfaces support Jumbo frames:

- Gigabit fiber and Gigabit copper ports in 9048GT and 9048GB.
- 10 Gigabit interfaces in 9024XL.
- IPv6—if you enable IPv6 Jumbo frame support you must configure the port interface MTU size to 9600 bytes.

The following control plane applications do not support Jumbo frames of 9600 bytes:

- Ping
- Telnet
- Domain Name Service (DNS)
- Secure Shell (SSH)
- Secure Copy Protocol (SCP)
- Simple Network Management Protocol (SNMP)
- Open Shortest Path First (OSPF) versions 2 and 3
- Routing Internet Protocol (RIP)

If you enable Jumbo frame support on the chassis, you must configure the port interfaces that support the Jumbo frames feature to an MTU size of 9600 bytes. Retain the default MTU size of 1950 bytes on port interfaces that do not support the Jumbo frames feature. Changes that you make to the MTU size take effect immediately.

SynOptics Network Management Protocol

Avaya Virtual Services Platform 9000 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.

Chapter 9: Chassis operations configuration using ACLI

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

Enabling the CPU-High Availability mode

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Enable CPU-High Availability (HA) mode to enable devices with two CPUs to recover quickly from a failure of the master CPU.

Procedure

1. Configure the following boot flag on the master CPU:

   boot config flags ha-cpu

   After you enable CPU-HA mode on the master CPU, the secondary CPU automatically resets to load settings from the previously-saved configuration file.
2. Type **y** after the following prompt appears:

   ```
   Do you want to continue (y/n) ?
   ```

   Responding to the user prompt with a **y** causes the secondary CPU to reset itself automatically, and that secondary CPU restarts with HA mode enabled.
3. Save the configuration

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Enable CPU-High Availability (HA) mode:

```
VSP-9012:1(config)#boot config flags ha-cpu
```

Cause the secondary CPU to reset itself with HA mode enabled:

```
VSP-9012:1(config)# Do you want to continue (y/n)?y
VSP-9012:1(config)#save config
```

Disabling CPU High Availability mode

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Perform this procedure to disable CPU-HA mode.

Procedure

Enter the following boot flag command on the master CPU:

```
no boot config flags ha-cpu
```

After you disable CPU-HA mode on the master CPU, the secondary CPU automatically resets to load settings from the previously-saved configuration file.

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Disable CPU-HA mode:

```
VSP-9012:1(config)#no boot config flags ha-cpu
```

Removing a master CP module with CPU-HA mode activated

Perform this procedure, if the system operates in CPU-HA mode, to properly remove the master CP module. You must perform this procedure to avoid jeopardizing the integrity of the file system.

Procedure

1. Log on to Global Configuration mode:
   ```
   enable
   ```

```
configure terminal
```

2. Use the `sys action cpu-switch-over` command to fail over to another CP.
3. Use the slot power commands to power down the module.
4. Remove the CP module.
   This action removes the original master.

   Important:

   Do not reinsert a CP module until at least 15 seconds have elapsed. This is long enough for another CP module to become master.

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#sys action cpu-switch-over
```

Enabling jumbo frames

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

Procedure

Enable jumbo frames:

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

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Enable jumbo frames to 9600 bytes:

```
VSP-9012:1(config)#sys mtu 9600
```

Variable definitions

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

Table 39: 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 CP Limit

Before you begin

- You must log on to Interface Configuration mode in ACLI for the port or MLT.

About this task

Configure CP Limit functionality to protect the switch from becoming congested by excess data flowing through one or more ports.

Procedure

1. Configure CP Limit on a port:
   `cp-limit [port {slot/port[-slot/port][,...]}] <1000-20000> [shutdown]`
2. Configure CP Limit on an MLT:
   `cp-limit <1000-20000> [shutdown]`

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Log on to GigabitEthernet Interface Configuration mode:

```
VSP-9012:1(config)#interface GigabitEthernet 3/14
```

Configure CP Limit on a port to 1000 packets per second and enable shutdown of the port:

```
VSP-9012:1(config-if)#cp-limit port 3/14 1000 shutdown
```

Variable definitions

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

Table 40: Variable definitions

Variable	Value
<1000–20000>	Configures the limit for control packets, expressed as packets per second (pps) in a range from 1000–20000. The default value is 8000. To set this option to the default value, use the default operator with the command.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
shutdown	Enables the shutdown of the port.

Enabling power management

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity.

Procedure

1. Enable power management:
   ```
   sys power
   ```
2. Enable power to a specified slot:
   ```
   sys power slot {slot[-slot][,...]}
   ```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Enable power management:

```
VSP-9012:1(config)#sys power
```

Enable power to slots 1, 2 and 3:

```
VSP-9012:1(config)#sys power slot 1,2,3
```

Variable definitions

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

Table 41: Variable definitions

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-6), or a series of slots (3,5,6). The valid slots are: 1–12, SF1–SF6, or all.

Configuring slot priority

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Configure slot priority to determine which slots shut down if insufficient power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first) and interface slots shut down before Switch Fabric slots of the same priority.

Procedure

Configure slot priority:

```
sys power slot-priority {<3-12>|SF2|SF3|SF5|SF6} {high|low}
```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Configure slot priority to determine that slot 3 has a high priority if insufficient power is available:

```
VSP-9012:1(config)#sys power slot-priority 3 high
```

Variable definitions

Use the data in the following table to use the `sys power slot-priority` command.

Table 42: Variable definitions

Variable	Value
<3–12>|SF2|SF3|SF5|SF6}	Designates the slot for priority setting. You can configure priority for the interface module slots (3–12) or for Switch Fabric slots 2, 3, 5, and 6.
high|low	Specifies slot priority.

Configuring port lock

Before you begin

- You must log on to Global Configuration mode in the ACLI.

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. Enable port lock globally:
   ```
   portlock enable
   ```
2. Log on to GigabitEthernet Interface Configuration mode:
   ```
   interface gigabitethernet {slot/port[-slot/port][,...]}
   ```
3. Lock a port:
   ```
   lock port {slot/port[-slot/port][,...]} enable
   ```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Log on to GigabitEthernet Interface Configuration mode:

```
VSP-9012:1(config)#interface GigabitEthernet 3/14
```

Unlock port 3/14:

```
VSP-9012:1(config-if)#no lock port 3/14 enable
```

Variable definitions

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

Table 43: 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 44: Variable definitions

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

Configuring SONMP

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

Procedure

1. Disable SONMP:
   ```
   no autotopology
   ```
2. Enable SONMP:

```
autotopology
```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Disable SONMP:

```
VSP-9012:1(config)#no autotopology
```

Viewing the topology message status

Before you begin

- You must log on to User EXEC mode in ACLI.

About this task

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

Procedure

Show the contents of the topology table:

```
show autotopology nmm-table
```

Example

```
VSP-9012:1>show autotopology nmm-table

================================================================================
                                Topology Table
================================================================================
Local                                                                    Rem
Port  IpAddress       SegmentId MacAddress   ChassisType   BT  LS  CS    Port
--------------------------------------------------------------------------------
 0/0  192.0.2.34     0x000000  00247f9f6000   VSP9012     12  Yes HtBt  0/0
 1/1  192.0.2.5      0x00011c  0018b0392801   ERS5510-48T 12  Yes HtBt  1/28
 1/1  192.0.2.30     0x000101  00247fa173fd   VSP9012     12  Yes HtBt  1/1
 1/1  192.0.2.39     0x000101  32a8016403fd   VSP9012     12  Yes HtBt  1/1
 1/1  192.0.2.55     0x000101  00247fa1d3fd   VSP9012     12  Yes HtBt  1/1
 3/1  192.0.2.38     0x000402  0014c75950c1   ERS8606     12  Yes HtBt  4/2
 3/6  198.51.100.32  0x000406  00247fa17065   VSP9012     12  Yes HtBt  4/6
 3/7  198.51.100.32  0x000407  00247fa17066   VSP9012     12  Yes HtBt  4/7
 3/8  198.51.100.32  0x000408  00247fa17067   VSP9012     12  Yes HtBt  4/8
 3/14 203.0.113.34   0x00040d  0014c75f40cc   ERS8606     12  Yes HtBt  4/13
 3/23 192.0.2.32     0x000417  00247fa17076   VSP9012     12  Yes HtBt  4/23
 3/24 192.0.2.32     0x000418  00247fa17077   VSP9012     12  Yes HtBt  4/24
 3/25 192.0.2.33     0x00041a  0014c75950e1   ERS8606     12  Yes HtBt  4/26
 3/26 203.0.113.34   0x000419  0014c75f40e0   ERS8606     12  Yes HtBt  4/25
 3/27 192.0.2.32     0x00041b  00247fa1707a   VSP9012     12  Yes HtBt  4/27
```

```
 3/28 192.0.2.32     0x00041c  00247fa1707b   VSP9012     12  Yes HtBt  4/28
--More-- (q = quit)
```

Job aid

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

Table 45: 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.
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 9000 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 • 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.

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 navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System** tab.
4. Type the contact information in the **sysContact** field.
5. Type the system name in the **sysName** field.
6. Type the location information in the **sysLocation** field.
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.

Name	Description
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.
VirtualIpAddr	Configures the virtual IP address that is advertised by the primary CPU and stored in the switch configuration file.
VirtualNetMask	Configures the net mask of the virtual management IP address.
VirtualIpv6Address	Configures the virtual IPv6 address that is advertised by the primary CPU. and stored in the switch configuration file.
VirtualIPv6Prefix Length	Configures the length of the virtual IPv6 prefix entry.
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.
LastRunTimeConfigSaveToSlave	Displays the last run-time configuration saved to the standby device.
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: • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration

Name	Description
	• saveRuntimeConfigToSlave—saves the current run-time configuration to the standby CPU • loadLicense—loads a software license file to enable features
ActionGroup2	Can be following action: • resetIstStatCounters—resets the IST statistic counters
ActionGroup3	Can be the following action: • flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be one of the following actions: • softReset—resets the device without running power-on tests • cpuSwitchOver—switch control from one CPU to another
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 navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Chassis** tab.
4. Edit the necessary options.
5. 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 number of slots (or modules) this device can contain.
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 4096.
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.
UdpSrcByVirtualIpEnable	Enables or disables virtual IP as the User Datagram Protocol (UDP) source. The default is disabled.
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 navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. Select the system flags you want to activate.
5. Clear the system flags you want to deactivate.
6. 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.
MrouteStreamLimit	Activates or disables Mroute Stream Limit. The default is disabled.
ForceTrapSender	Configures circuitless IP as a trap originator. The default is disabled.
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.
ProfileType	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are: • balanced • unicastOptimized • multicastOptimized

Name	Description
	The default is balanced
Lossless8021p	Specifies the lossless-802.1p value. The range is 0 to 6. The default is 3. **Note:** The internal QoS level that corresponds to the lossless 802.1p value must be 3 .Avaya recommends that you do not use filters to remark the internal QoS level. When you enable lossless-PFC on a port, the port cannot become lossless-PFC if the lossless-802.1p value maps to an internal QoS level other than 3, or if the internal QoS level 3 maps to another 802.1p value. In a Lossless-PFC (802.1Qbb) domain, the lossless behavior is guaranteed as long as the Lossless 802.1p, ingress 1p to QoS map and the egress QoS to 1p map are consistent. When you change the Lossless 802.1p and ingress 1p to QoS map, you must configure the egress QoS to 1p map correctly.
HaCpu	Activates or disables the CPU High Availability feature. If you enable or disable High Availability mode, the secondary CPU resets automatically to load settings from the saved configuration file. The default is enable.
HaCpuState	Indicates the CPU High Availability state. • initialization—indicates the CPU is in this state • oneWayActive—modules that need to synchronize register with the framework (either locally or a message received from a remote CPU) • twoWayActive—modules that need to synchronize register with the framework (either locally or a message received from a remote CPU) • synchronized—table-based synchronization is complete on the current CPU • remoteIncompatible—CPU framework version is incompatible with the remote CPU • error—if an invalid event is generated in a specific state the CPU enters Error state • disabled—High Availability is not activated

Name	Description
	• peerNotConnected—no established peer connection • peerConnected—established peer connection is established • lostPeerConnection—lost connection to peer or standby CPU • notSynchronized—table-based synchronization is not complete
HaEvent	Indicates the High Availability event status. • restart—causes the state machine to restart. • systemRegistrationDone—causes the CPU to transfer to One Way or Two Way Active state. • tableSynchronizationDone—causes the CPU to transfer to synchronized state. • versionIncompatible—causes the CPU to go to remote incompatible state • noEvent—means no event occurred to date.
StandbyCpu	Indicates the state of the standby CPU.

Enabling CPU High Availability

About this task

Enable CPU high-availability (HA) mode to recover quickly from a failure of the master CPU on systems with two CPUs.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. In **HaCpu** section, select **Enable**.
5. Click **Apply**.
6. Click **Yes** on the confirmation screen.

   After you enable HA mode on the master CPU, the secondary CPU automatically resets to load settings from its previously-saved configuration file. You must manually reset the primary CPU while the secondary CPU starts.

Important:

Failure to manually start the primary CPU before the secondary finishes starting can lead to system instability. Traffic is interrupted after you manually reset the master.

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.
Descr	Displays the description of the port. A textual string containing information about the interface. This string should include the

Name	Description
	name of the manufacturer, the product name and the version of the hardware 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 on GBIC cards.
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	Enables or disables Autonegotiation for this port.
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.

Name	Description
OperSpeed	Displays the currently saved AdminSpeed value.
AutoNegAd	Configures the Custom Autonegotiation Advertisement (CANA) settings of the port. 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.) Any change in the value of this bit map will force the PHY to restart the auto-negotiation process. This will have the same effect as physically unplugging and reattaching the cable plant attached to ths port. 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. The default for this object will be all of the capabilities supported by the hardware.
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.
AdminRouting	Configures the port as routable or not. The default is enabled.

Name	Description
OperRouting	Displays the currently saved AdminRouting value.
HighSecureEnable	Enables or disables the high secure feature for this port.
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.
Action	Performs one of the following actions on the port • 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 • triggerRipUpdate - manually trigger a RIP update • clearLoopDetectAlarm - manually enable the port on all the disabled vlans. The default is none.
Result	Displays result of the selected action. The default is none.

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. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Boot Config** tab.

Boot Config field descriptions

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

Name	Description
Slot	Specifies the slot number of the boot device.
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time configuration.

Changing the boot configuration

About this task

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

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, VSP 9000 supports SSH server, remote login (rlogin) server and Remote Shell (rsh) server only. VSP 9000 does not support outbound SSH client over IPv6, rlogin client over IPv6 or rsh client over IPv6. On IPv4 networks, VSP 9000 supports both server and client for SSH, rlogin and rsh.

Procedure

1. In the Device Physical View tab, select a CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Boot** tab.
5. Select the services you want to enable.

6. Click **Apply**.

Boot field descriptions

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

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time image.
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	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. If you enable this flag, the switch does not restart following a fatal error. The default value is disabled. If you change this parameter, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
EnableHwWatchDogTimer	Activates or disables the hardware watchdog timer monitoring a hardware circuit. The default value is activated. The watchdog timer restarts the switch based on software errors. If you change the wdt flag, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.

Name	Description
EnableRebootOnError	Activates or disables automatic reboot on a fatal error. The default value is activated. The reboot command is equivalent to the debugmode command. If you change the reboot variable value, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled. If you disable the Telnet server service in a dual CPU system, the Telnet server prevents a Telnet connection initiated from the other CPU.
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. If you disable the TFTP server you can still copy files between the CPUs.
EnableSshServer	Activates or disables the SSH server service. The default value is enabled.

Enabling Jumbo frames

About this task

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

Procedure

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

5. 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. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **User Set Time** tab.
4. Type the correct details.
5. Click **Apply**.

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.

Configuring CP Limit

About this task

Configure CP Limit functionality to protect the switch from becoming congested by an excess of data flowing through one or more ports.

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 **CpLimitShutDownEnable** for the CP Limit option.
6. Click **Apply**.

CP Limit field descriptions

Use the data in the following table to use the **CP Limit** tab.

Name	Description
CpLimitPktRate	Limits control packets on the port to QoS levels 6 and 7. Sets the limit to packets per second. The range is 1000 to 20000. The default value is 8000.
CpLimitShutDownEnable	Activates or disables the CP Limit feature. The default is disabled.
AutoRecoverPort	Activates or disables auto recovery of the port from action taken by CP Limit, link flap, or loop detect features. The default value is disabled.

Assigning an IP address for the management port

Before you begin

- You must make a direct connection through the console port to configure a new IP address. If you connect remotely, you can view or delete the existing IP address configuration. If you delete the IP address remotely, you lose the EDM connection to the device.

About this task

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **VRF Context View**.
2. Click **Set VRF Context View**.
3. Select **MgmtRouter**, VRF 512.
4. Click **Launch VRF Context View**.

   A new EDM Web page appears for the VRF context. Parameters that you cannot configure for this context appear dim.
5. In the Device Physical view, select the management port on the CP module.
6. In the navigation tree, open the following folders: **Configuration** > **Edit**.
7. Click **Mgmt Port**.
8. Click the **IP Address** tab.
9. Click **Insert**.
10. Configure the IP address and mask.
11. Click **Insert**.
12. Close the VRF context view.

IP Address field descriptions

Use the data in the following table to use the **IP Address** tab.

Name	Description
Interface	Specifies the slot and port for the management port.
Ip Address	Specifies the IP address for the management port.
Net Mask	Specifies the subnet mask for the IP address.
BcastAddrFormat	Specifies the broadcast address format for the management port.
ReasmMaxSize	Specifies the size of the largest IP datagram that can be reassembled from IP fragmented datagrams received on the management port.
VlanId	Specifies the VLAN ID to which the management port belongs.
BrouterPort	Specifies if the management port is a brouter port rather than a routeable VLAN. This value cannot be changed after the row is created.
MacOffset	Translates the IP address into a MAC address.

Editing the management port parameters

About this task

The management port on the CP module is a 10/100 Mb/s Ethernet port that you can use for an out-of-band management connection to the switch.

If you use EDM to configure the static routes of the management port, you do not receive a warning if you configure a non-natural mask. After you save the changes, the system deletes those static routes after the next restart, possibly causing the loss of IP connectivity to the management port.

If you are uncertain whether the mask you configure is non-natural, use ACLI to configure static routes.

Procedure

1. In the Device Physical View tab, select the management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **General** tab.

5. Modify the appropriate settings.
6. Click **Apply**.

General field descriptions

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

Name	Description
Index	Specifies the slot and port number of the management port.
AdminStatus	Configures the administrative status of the device as up (ready to pass packets) or down. The testing state indicates that no operational packets can be passed.
OperStatus	Specifies the operational status of the device.
Mtu	Shows the configuration for the maximum transmission unit. The size of the largest packet which can be sent/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.
LinkTrap	Enables or disables traps for the link status.
PhysAddress	Shows the MAC address.
AutoNegotiate	Activates or disables auto-negotiate.
AdminDuplex	Specifies the administrative duplex mode for the management port. The default is half.
OperDuplex	Specifies the operational duplex configuration for this port.
AdminSpeed	Specifies the administrative speed for this port. The default is 10 Mb/s.
OperSpeed	Shows the current operating data rate of the port.

Configuring the management port IPv6 interface parameters

About this task

Configure IPv6 management port parameters to use IPv6 routing on the port.

Procedure

1. In the Device Physical View tab, select the management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **IPv6 Interface** tab.
5. Click **Insert**.
6. Edit the fields as required.
7. Click **Insert**.
8. Click **Apply**.

IPv6 Interface field descriptions

Use the data in the following table to use the **IPv6 Interface** tab.

Name	Description
IfIndex	Identifies the unique IPv6 interface.
Descr	Specifies a textual string containing information about the interface. The network management system also configures the **Descr** string.
Type	Specifies the type of interface.
ReasmMaxSize(MTU)	Configures the MTU for this IPv6 interface. This value must be the same for all the IP addresses defined on this interface. The default value is 1500.
PhysAddress	Specifies the physical address for the interface. For example, for an IPv6 interface attached to an 802.x link, this value is a MAC address.
AdminStatus	Configures the indication of whether IPv6 is activated (up) or disabled (down) on this interface. This object does not affect the state of the interface, only the interface connection to an IPv6 stack. The default is false (cleared).
ReachableTime	Configures the time, in milliseconds, that the system considers a neighbor reachable after it receives a reachability confirmation. The value is in a range from 0–3600000. The default value is 30000.
RetransmitTimer	Configures the time between retransmissions of neighbor solicitation messages to a neighbor; during

Name	Description
	address resolution or neighbor reachability discovery. The value is expressed in milliseconds in a range from 0–3600000. The default value is 1000.
CurHopLimit	Specifies the current hop limit field sent in router advertisements from this interface. The value must be the current diameter of the Internet. A value of zero indicates that the advertisement does not specify a value for the current hop limit. The default is 64.

Configuring management port IPv6 addresses

About this task

Configure management port IPv6 addresses to add or remove IPv6 addresses from the port.

Avaya supports IPv6 addressing with Ping, Telnet, and SNMP.

Procedure

1. In the Device Physical View tab, select the management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **IPv6 Addresses** tab.
5. Click **Insert**.
6. In the **Addr** box, type the required IPv6 address for the management port.
7. In the **AddrLen** box, type the number of bits from the IPv6 address you want to advertise.
8. Click **Insert**.
9. Click **Apply**.

IPv6 Addresses field descriptions

Use the data in the following table to use the **IPv6 Addresses** tab.

Name	Description
IfIndex	Specifies an index value which uniquely identifies the interface.

Name	Description
Addr	Specifies the IPv6 address to which this entry addressing information pertains. If the IPv6 address exceeds 116 octets, the object identifiers (OIDS) of instances of columns in this row is more than 128 subidentifiers and you cannot use SNMPv1, SNMPv2c, or SNMPv3 to access them.
AddrLen	Specifies the prefix length value for this address. You cannot change the address length after creation. You must provide this field to create an entry in this table.
Type	Specifies Unicast, the only supported type.
Origin	Specifies the origin of the address. The origin of the address can be one of the following: other, manual, dhcp, linklayer, or random.
Status	Specifies the status of the address, describing if the address can be used for communication. The status can be one of the following: preferred, deprecated, invalid, inaccessible, unknown, tentative, or duplicate.
Created	Specifies the time this entry was created. If this entry was created prior to the last initialization of the local network management subsystem, then this option contains a zero value.
LastChanged	Specifies the time this entry was last updated. If this entry was updated prior to the last initialization of the local network management subsystem, then this option contains a zero value.

Creating IPv6 static routes

About this task

To improve the static route management, you can change static routes directly with the IPv6 static routing table manager. The static routing table is separate from the system routing table, which the router uses to control forwarding. Although the tables are separate, entries in the static routing table manager automatically change in the system routing table if the next-hop address in the static route is reachable and the static route is enabled.

Use static routes to manually configure routes to destination IPv6 address prefixes.

Procedure

1. In the Device Physical View, select the management port on the CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.

3. Click **Mgmt Port**.
4. Click the **Static Routes** tab.
5. Click **Insert**.
6. In the **Dest** box, type the IPv6 address.
7. In the **PrefixLength** box, type the length of the prefix for the IPv6 address.
8. In the **NextHop** box, type the IPv6 address of the router through which the specified route is accessible.
9. In the **Cost** box, type a number for the distance.
10. Select the **Enable** check box.
11. Click **Insert**.

Static Routes field descriptions

Use the data in the following table to use the **Static Routes** tab.

Name	Description
IfIndex	Specifies the interface to which this entry applies. This parameter is used only if the next hop is a link-local address.
Dest	Specifies the IPv6 destination network address.
PrefixLength	Specifies the number bits you want to advertise from the prefix. The range is 0 to 128.
NextHop	Specifies the IPv6 address of the next hop on this route.
Cost	Specifies the cost or distance ratio to reach the destination for this node. The range is 1-65535. The default value is 1.
Enable	Enables the static route on the port. The default value is enable.
Status	Indicates the current status of this entry. The default value is active.
Preference	Specifies the routing preference of the destination IPv6 address. The range is 1-255. The default value is 5.

Editing serial port parameters

About this task

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

Procedure

1. In the Device Physical View tab, select the console port on the CP module.
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. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. 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 power information for specific components

About this task

View power information for specific components to identify the power use by each module in the chassis.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Power Consumption** tab.

Power Consumption field descriptions

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

Name	Description
Index	Shows the slot number.
PowerStatus	Shows the current power state for the slot.
SlotDescription	Shows the type and location of slot in the chassis.
CardDescription	Shows the type of hardware component in the slot.
PowerPriority	Shows the priority of the slot for power management.
BasePower	Shows the base power required for the slot.
ConsumedPower	Shows the actual consumed power for the slot. This value is zero if the power status is off.

Configuring slot priority

About this task

Configure slot priority to determine which slots shut down if not enough power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down by highest slot number first.

To configure slot priority for slots at the back of the chassis, you must use ACLI.

Procedure

1. In the Device Physical View tab, select a module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Card** tab.
5. In the **PowerManagementPriority** box, select the priority level.
6. Click **Apply**.

Viewing fan information

About this task

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

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Fan Zone** tab.

Fan Zone field descriptions

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

Name	Description
Type	Shows if the fan zone is at the front of the chassis or the rear of the chassis.
Mode	Shows the mode of the fan zone, either normal or alarm.
ModeStatus	Shows the alarm type as one of the following: • normal • fanFault • alarmThresholdExceeded
AlarmTimer	Shows the remaining time before the system check and module shutdown if the fan is in the alarm state. This value is zero if the fan is not in an alarm state.
Temperature	Shows the highest temperature, measured in Celsius, from all sensors in the zone.

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.

Name	Description
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.

Name	Description
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 • topChanged—Topology information recently changed. • heartbeat—Topology information is unchanged. • new—The sending agent is in a new state.

Chapter 11: 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 or hot swap detection.
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.
Enable	Detects the hot swap of installed modules. The default is disabled.
Detection per Status Poll Intervals	Specifies the number of poll intervals for detection, if enabled. The default is 2 intervals.

Viewing module information

About this task

View the administrative status for modules in the front of the chassis.

Procedure

1. In the Device Physical View tab, select an interface or CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Card** tab.

Card field descriptions

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

Name	Description
CardType	Displays the model number of the module.
CardDescription	Shows a description of the installed module.
CardSerialNo	Shows the serial number for the installed module.
CardPartNo	Shows the part number.
CardAssemblyDate	Shows the date the module was assembled.
CardHWConfig	Shows the hardware revision.
AdminStatus	Changes the administrative status for the module.
OperStatus	Shows the operational status for the module.
ModuleType	Indicates the encoded value for the module type
ModuleDescription	Displays the model number of the module.
ModuleSerialNo	Displays the serial number of the module.
ModulePartNo	Displays the part number of the module.
ModuleDateCode	Displays the manufacturing date code for the module.
ModuleHWConfig	Displays the hardware version.
PowerManagementPriority	Changes the slot priority for power management.

Name	Description
SlotPower	Administratively turns power on or off for the slot.

Viewing Switch Fabric module information

About this task

View the administrative status for Switch Fabric modules in the back of the chassis.

Procedure

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

Switch Fabric field descriptions

Use the data in the following table to use the **Switch Fabric** tab.

Name	Description
Index	Shows a unique value for each module within the chassis. This value is determined by the chassis slot number where the module is inserted.
CardType	Indicates the module type.
CardDescription	Shows a description for the module.
AdminStatus	Changes the administrative status for the module.
OperStatus	Shows the operational status for the module.
ModuleType	Indicates the encoded value for the module type.
ModuleSerialNo	Displays the serial number of the module.
ModulePartNo	Displays the part number of the module.
ModuleDateCode	Displays the manufacturing date code for the module.
PowerManagementPriority	Changes the slot priority for power management.
SlotPower	Turns power on or off for the module.

Viewing fan details

About this task

View read-only information about the operating status of the fans in the cooling modules.

Procedure

1. In the Device Physical View tab, select a cooling module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Fan**.
4. Click the **Fan Detail** tab.

Fan Detail field descriptions

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

Name	Description
Type	Indicates the fan type.
Tray	Displays the number of trays for each zone in the chassis.
Fan	Displays the number of fans for each tray.
ExpectedSpeed	Displays the administrative configuration for the fan speed: • low: configured by software • medium: configured by software • high: configured by software • hardware: controlled by hardware
OperSpeed	Displays the actual fan speed.
Status	Displays the operational status of the fan: • ok: operating under normal conditions • faulty: not operating as expected

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: • on (up) • off (down)
InputLineVoltage	Specifies the input line voltage. Two possible states exist: • low 110v—power supply connected to a 110 Volt source • high 220v—power supply connected to a 220 Volt source If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage shows the low 110v value.

Name	Description
OutputWatts	Displays the output power of this power supply.

Viewing ASIC information for interface modules

About this task

Perform this procedure to view information about the application-specific integrated circuit (ASIC) installed on an interface module.

Procedure

1. In the Device Physical View tab, select an interface module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **ASIC** tab.

ASIC field descriptions

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

Name	Description
CardType	Indicates the card type.
K2Fpga	Indicates the Kuma 2 (K2) field-programmable gate array (FPGA) version for the interface module.
IoDateDC	Indicates the IO Date DC complex programmable logic device (CPLD) for the interface module.
IoDateBB	Indicates the IO Date BaseBoard CPLD for the interface module.
IoPimCpld	Indicates the IO PIM CPLD for the interface module.
Led0Cpld	Indicates the LED0 CPLD for the interface module.
Led1Cpld	Indicates the LED1 CPLD for the interface module.

Name	Description
ZagrosFpga	Indicates the Zagros FPGA for the interface module.
Rsp	Indicates the RSP for the interface module.
BcmMac	Indicates the BCM MAC for the interface module.
QE	Indicates the QE version for the interface module.

Viewing module temperatures on the chassis

About this task

You can view information about the temperature of each module on the chassis.

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

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

To avoid fan speed fluctuation and repeated alarms, the fan speed and fan speed indicator do not return to normal until the zone temperature on the module is at least 10 degrees Celsius below the threshold temperature.

Procedure

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

Temperature field descriptions

Use the information in the following table to help you understand the **Temperature** tab.

Name	Description
SlotIndex	Specifies the slot number of

Name	Description
	• a Control Processor (CP) module (slots 1 and 2) • an Input/Output (IO) module (slots 3–12) • a Switch Fabric (SF) module (slots 21–26)
SlotDescription	Specifies the slot type information; for example: Slot1, Slot12, SF1, or SF4.
Zone1Temperature	Specifies the Zone 1 temperature on the module in the specified slot, measured in degrees Celsius. If there is no value in this Temperature tab table cell this zone does not exist on the module in the slot.
Zone2Temperature	Specifies the Zone 2 temperature on the module in the specified slot , measured in degrees Celsius. If there is no value in this Temperature tab table cell this zone does not exist on the module in the slot.
Zone3Temperature	Specifies the Zone 3 temperature on the module in the specified slot, measured in degrees Celsius. If there is no value in this Temperature tab table cell this zone does not exist on the module in the slot.
Zone4Temperature	Specifies the Zone 4 temperature on the module in the specified slot, measured in degrees Celsius. If there is no value in this Temperature tab table cell this zone does not exist on the module in the slot.
Zone5Temperature	Specifies the Zone 5 temperature on the module in the specified slot , measured in degrees Celsius. If tehre is no value in this Temperature tab table cell this zone does not exist on the module in the slot.
HighTemperature	Specifies the highest temperature, measured in degrees Celsius.
LowTemperature	Specifies the lowest temperature, measured in degrees Celsius.
AlarmThreshold	Specifies the temperature, in degrees Celsius, that provokes an alarm.
ShutdownThreshold	Specifies the temperature, in degrees Celsius, that initiates a shutdown.

Viewing ASIC information for CP modules

About this task

View information about the application-specific integrated circuit (ASIC)installed on a Control Processor (CP) module.

Procedure

1. In the Device Physical View tab, select a CP module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **CP-ASIC** tab.

CP-ASIC field descriptions

Use the data in the following table to use the **CP-ASIC** tab.

Name	Description
CardType	Indicates the card type.
OxateCpld	Indicates the Oxate CPLD version for the CP module.
OxideFpga	Indicates the Oxide FGPA version for the CP module.
CatskillFpga	Indicates the Catskill FPGA version for the CP module.
QE	Indicates the QE version for the CP module.

Chapter 12: DNS fundamentals

This section provides conceptual material on the Domain Name Service (DNS) implementation for Avaya Virtual Services Platform 9000. 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 an 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.

In non-High Availability (HA) mode, you can configure a separate DNS server for master and secondary CP modules. In HA mode, you can configure a DNS server only from the master CP module.

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.

Avaya does not provide a default hosts file on the system, but Avaya supports the local host look up feature. If you want to use the local host look up feature, you can create it. The format is the same as a Uniplexed Information and Computing Service (UNIX) workstation. Use the editor provided on the system to create, save, or modify such a file.

IPv6 Support

The Domain Name Service (DNS) used by the Avaya Virtual Services Platform 9000 supports both IPv4 and IPv6 addresses. There is no difference in functionality or configuration.

Chapter 13: 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 and IPv6 addresses with no difference in functionality or configuration using ACLI.

Configuring the DNS client

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Configure the Domain Name Service to establish the mapping between an IP name and an IPv4 address or IPv6 address. DNS supports IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.

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. Configure the DNS client:
   ```
   ip domain-name WORD<0-255>
   ```
2. Optionally, add addresses for additional DNS servers:
   ```
   ip name-server <primary|secondary|tertiary> WORD<0-46>
   ```
3. View the DNS client system status:
   ```
   show ip dns
   ```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Add addresses for additional DNS servers:

```
VSP-9012:1(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 46: Variable definitions

Variable	Value
WORD<0–255>	Configures the default domain name. *WORD<0–255>* is a string 0–255 characters.

Use the data in the following table to use the `ip name-server` command.

Table 47: Variable definitions

Variable	Value
primary|secondary|tertiary *WORD<0–46>*	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) for IPv6. You can specify the IP address for only one server at a time; you cannot specify all three servers in one command. Use the no operator before this parameter, `no ip name-server <primary|secondary|tertiatry>`

Querying the DNS host

Before you begin

- You must log on to Privileged EXEC mode in ACLI.

About this task

Query the DNS host for information about host addresses.

You can enter either a hostname, an IPv4 address or IPv6 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 and IPv6 addresses with no difference in functionality or configuration using ACLI.

Procedure

View the host information:

```
show hosts WORD<0-256>
```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

View the host information:

```
VSP-9012:1(config)#show hosts 4717::7933:1
```

Variable definitions

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

Table 48: Variable definitions

Variable	Value
WORD<0–256>	Specifies one of the following: • 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. • the IPv6 address of the host DNS server in hexadecimal format (string length 0–46).

Chapter 14: DNS configuration using EDM

This section describes how to configure the Domain Name Service (DNS) using Enterprise Device Manager (EDM).

DNS supports IPv4 and IPv6 addresses with no difference in functionality or configuration except for the following. Under the **DNS Servers** tab, in the **DnsServerListAddressType** box, you must select **ipv4** or **ipv6**.

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 and IPv6 addresses with no difference in functionality or configuration except for the following. Under the **DNS Servers** tab, in the **DnsServerListAddressType** box, you must select **ipv4** or **ipv6**.

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 or IPv6.
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 or IPv6 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 and IPv6 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 or the IPv6 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, the host IPv4 address or the host IPv6 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 15: Licensing fundamentals

This section provides conceptual information about feature licensing for Avaya Virtual Services Platform 9000. Review this section before you make changes to the license configuration.

Feature licensing

Enabling features on Virtual Services Platform 9000 requires the generation and installation of a license file that contains the authorized MAC addresses of the switches on which you install the license file.

In addition to a Base Software License, Virtual Services Platform 9000 supports optional Advanced and Premier feature licenses to provide access to additional features contained within those licensing levels. Purchase these licenses separately in the form of either an Advanced License Kit or Premier License Kit. The Premier License Kit contains all Advanced License Kit features. When you purchase either an Advanced License Kit or a Premier License Kit, the license covers all current and future features. If you currently have an Advanced License Kit, no discounted price exists to move to a Premier License Kit; you must purchase a complete Premier License Kit. If you purchase a Premier License Kit, you have licenses for all features for the life of the product. For more information, contact your Avaya sales representative.

Advanced and Premier License level features use a software-based licensing mechanism to unlock specific features.

All licensing activities are performed through the Avaya Data Licensing Portal at http://avayadatalicensing.com.

Base License

The Base License activates the features not included in either the Advanced or Premier Licenses.

Advanced License

The Advanced License activates the following features in addition to the Base License:

- Border Gateway Protocol version 4 (BGP4) for 16 peers or 64 000 routes
- Packet Capture function (PCAP)
- Layer 3 mirroring
- IPv6 routing

Premier License

The Premier License activates the following features in addition to the Advanced License:

- Lossless Ethernet
- Virtual Routing and Forwarding (VRF)
- 1.5 million IP routes, 500 000 IP FIB entries
- 256 BGP peers
- Shortest Path Bridging MAC (SPBM)

The Premier License activates all licensed features on Virtual Services Platform 9000.

Important:

Avaya recommends that you purchase the Premier License if you anticipate growth in your network. If you purchase the Advanced License, and later require features available only if you have the Premier License, you must also purchase the Premier License. If you purchase the Premier License initially, you have access to all features enabled by the Advanced License and the Premier License (you do not need to purchase the Advanced License separately).

You must purchase the Base License for each chassis. You can install an Advanced or Premier License on each chassis after you install the Base software license, but the Advanced and Premier Licenses are optional.

Premier Trial License

Virtual Services Platform 9000 provides a trial period of 60 days during which you have access to all features. In the trial period you can configure all features without restriction, including system console and log messages.

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 Advanced/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.

License type and part numbers

The following table provides the part number for the various licenses supported on Virtual Services Platform 9000.

Table 49: Supported licenses

Part number/ Order code	License type	Number of chassis supported
EC1410010	Advanced License Kit for one chassis. (One license required for each chassis.)	1
EC1410015	Premier License kit for one chassis. (One license required for each chassis.)	1

License certificates

Each Advanced or Premier License Kit contains a License Certificate with a License Authorization Code (LAC) that permits a specific number of licenses for one or multiple Virtual Services Platform 9000 systems. Each system requires and uses one license file to unlock features associated with that license. A single license file can contain up to 100 Base MAC addresses for installation on multiple systems.

The License Certificate provides printed instructions about how to deposit license entitlements (LACs) into a license bank, enter switch base MAC addresses, and create the license file. The License Certificate also includes instructions about how to copy the license file onto each switch to unlock additional features associated with a license.

License file generation

After you purchase a license, you must generate the license file using the Avaya Electronic Licensing portal. The licensing portal works on the concept of a license bank—an electronic repository for all license entitlements and licenses. The portal deposits license entitlements into your license bank after you enter an LAC. The LAC is on the License Certificate you receive after you purchase the license.

The software license file uses authorized chassis base MAC addresses. You can generate an individual license file with one or multiple chassis base MAC addresses. You can add additional MAC addresses to the same license file at a later time, if required. A license file can support up to 100 unique MAC addresses.

Feature license files

After you obtain the license file to enable Advanced or Premier License features, you must install the license file on the system to unlock the associated licensed features. For Virtual

Services Platform 9000, you must load a license file on the internal flash of the Control Processor (CP) module.

License transfer

For information about how to transfer a license and obtain an updated license file for Virtual Services Platform 9000, see License generation and transfer on page 161.

Licensing

Generate and install license files to enable advanced and premier features on Avaya Virtual Services Platform 9000.

This work flows shows you the sequence of tasks you perform to configure licensed features.

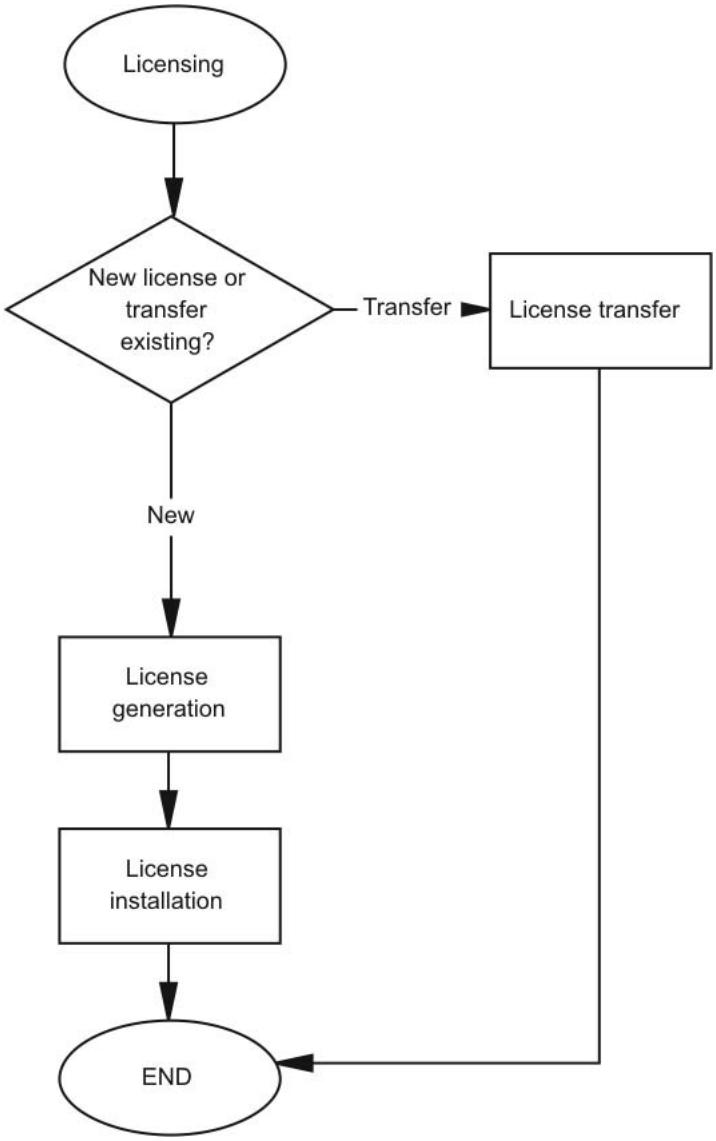

Figure 2: Licensing tasks

Before you begin

- You must purchase the appropriate license for the additional switch features. For more information, contact your Avaya sales representative.

Chapter 16: License generation and transfer

Generate the license file you need to enable licensed features on the system. This task is independent of loading the license file on the system.

Transfer a license and obtain an updated license file for Avaya Virtual Services Platform 9000.

Generating a license

Before you begin

- You must purchase a Virtual Services Platform 9000 license kit that contains a License Certificate with a License Authorization Code (LAC).

About this task

Generate a license to enable licensed features on the system.

Use the data in the following table to use the Generate license screen.

Table 50: Variable definitions

Variable	Value
Switch MAC Address	Specifies the base MAC address of the switch for which to generate the license file. Follow the example format that appears next to the entry box.
File Name of List of MAC Addresses	Specifies the file name that contains multiple base MAC addresses of the switches for which to generate the license file. The file must be an ASCII text file and adhere to the following rules: • Each line must contain one MAC address (use MS-DOS or UNIX line ending characters. • The MAC addresses can be in lower or upper case characters and must be in hexadecimal format with each pair (byte) separated by colons (XX:XX:XX:XX:XX:XX).

Variable	Value
	• Do not use other characters or spaces. • The file must contain the correct base MAC addresses. Incorrect addresses result in non-working licensed features. • The number of MAC addresses must not exceed the number of licenses allowed for the License Authorization Code.
Output License File Name	Specifies the name of the license file. The file name is limited to 64 alphanumeric, lowercase characters. You can use the underscore (_) character. Do not use spaces, dashes, or special characters. The filename must use a dot (.) with the file extension .dat. For example, license.dat. **Important:** While you can use the Avaya Licensing portal to generate a license file using your choice of filename or extension, Virtual Services Platform 9000 searches for a license filename with an extension of .dat in the internal flash directory. Therefore, you need to ensure the destination license file you copy to the device uses .dat as the file extension. Failure to do this results in unavailable Advanced or Premier features.
User Comment 1	Provides a location for free-form, user-entered text related to the license file. For example, a location to assist in asset tracking.
User Comment 2	Provides a second location for free-form, user-entered text related to the license file. For example, a location to assist in asset tracking.

Procedure

1. Obtain the base MAC address for the chassis:
   ```
   show sys-info
   ```
2. Go to the Avaya Electronic Licensing portal at http://www.avayadatalicensing.com.
3. Type your contact information in the required boxes.

4. Create a new license bank or provide details for an existing license bank to deposit licenses.
5. Select an email notification option. The system sends newly generated licenses to the nominated email address.
6. Enter the License Authorization Code provided on the License Certificate when you purchased the license.
7. Click **Submit**.

   A new screen appears while the portal activates and deposits the associated number of licenses in the license bank. Do not leave the page or close your Web browser. Upon successful completion, a confirmation message appears.
8. Click **Go to License Bank to Download license**.

   The License Bank screen appears and provides information about the License Authorization Code just activated.
9. Click **Generate License**.

   The Generate License screen appears.
10. Enter the required details for the license file.
11. Click **Generate License File**.

    A confirmation message appears. The license file is immediately sent to the nominated email address set up with the license bank. You can choose to return to the license bank or log out from the licensing portal.

Important:

The license file is a compressed binary file. Ensure that while downloading or saving this file, the browser does not automatically decompress this file.

Job aid

The following example shows partial information that appears after you use the **`show sys-info`** command to view the base MAC address.

```
VSP-9012:1#show sys-info

General Info :

        SysDescr     : VSP-9012 (3.2.0.0) (GA)
        SysName      : CB-SWA
        SysUpTime    : 0 day(s), 06:55:25
        SysContact   : http://support.avaya.com/
        SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis            : 9012
        Serial#            : SAN1223008S
```

```
        H/W Revision       :
        H/W Config         :
        NumSlots           : 12
        NumPorts           : 50
        BaseMacAddr        : 00:24:7f:9f:60:00
        MacAddrCapacity    : 4096
        MgmtMacAddr        : 00:24:7f:9f:63:fd
        System MTU         : 1950

Card Info :


--More-- (q = quit)
```

Transferring a license

About this task

You need to transfer a license in the following scenarios:

- Due to a chassis failure, you replaced the platform with a replacement chassis that has a new base MAC address.
- You entered an incorrect base MAC address on the Avaya Electronic Licensing portal during the license file generation process.
- You need to transfer the license to a different platform.

Procedure

1. Find the base MAC address of the new chassis:
   ```
   show sys-info
   ```
2. Go to the Avaya Electronic Licensing portal at http://www.avayadatalicensing.com.
3. Click **License Bank** on the left menu.
4. Login to the License Bank by entering the License Bank name and password.
5. Select the appropriate License Authorization Code (LAC) entry in the License Bank associated with the license type, and then click **View Details**.

   A License Bank can contain many different License types for different products. Therefore, it is important that you select the correct LAC entry for the product and license type to access the license file that contains the MAC address you want to replace. For example, if the base MAC address that you want to replace uses a Premier License, select a Premier Licence LAC to view the transaction for the license file that contains the base MAC.
6. Within the View Details screen, select a transaction that has the license file name in use on the chassis that you want to replace.

The same license file name can appear in several transactions; choose a transaction that has the license file name that you need to replace. The license file always contains the latest full list of MAC addresses.

7. Click **Replace Switch**.

   The Replace Switch MAC screen appears and shows the name of the license file and the MAC addresses that it contains.

8. In the Enter Replacement Switch MAC Address box, type the new base MAC address.

9. In the Select the Switch MAC Address to replace list, select the MAC address that you want to replace.

   Before you proceed to the next step, ensure that you select the correct MAC address to replace, and that the new base MAC address is correct.

10. Click **Replace Switch MAC**.

    A screen appears that confirms the MAC address replacement. The license file is immediately updated, however it is not sent to the nominated License Bank email address.

    If the MAC replacement limit reaches for the LAC, a message appears and the MAC replacement fails. If this situation occurs, you must repeat this procedure with a different LAC entry in the License Bank. If no other LAC entries exist in the License Bank, contact Avaya Technical Support.

11. Click **Return to License Bank Details**.

12. Locate the transaction with the license file that is updated with the new MAC address, and then click **Download**.

    A File Download window appears.

13. Click **Save**.

    You can save the license file on the PC you use to access the license portal. After you download the license file, you need to install it on the new chassis.

Chapter 17: License installation using ACLI

Install and manage a license file for Avaya Virtual Services Platform 9000 by using the Avaya command line interface (ACLI).

Installing a license file

Before you begin

- You must log on to the Global Configuration mode in ACLI.
- You must store the license file on a Trivial File Transfer Protocol (TFTP) server. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
- Ensure that you have the correct license file with the base MAC address of Virtual Services Platform 9000 on which you need to install the license. Otherwise, the system does not unblock the licensed features.
- If the chassis uses two CP modules, you do not need to install the license file on the secondary CP module. After you enable High Availability, the primary CP module copies the license vectors to the secondary CP module during table sync and the trial period countdown is stopped. This action ensures that the run time vectors of the primary and secondary CP module are the same. After you save the configuration on the primary CP module, the system copies the license file to the secondary CP module.

  In warm-standby mode, the system does not synchronize license vectors with the secondary CP module. However, the system copies the license file to the secondary CP module after you save the configuration with the save to standby flag configured as true.

About this task

Install a license file on Avaya Virtual Services Platform 9000 to enable licensed features.

Procedure

1. Install a license file:

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

   ```
   copy <x:x:x:x:x:x:x:x>:<srcfile> /intflash/<destfile>
   ```

2. Load the license file:

   ```
   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.

3. Save the configuration.

Example

Copy a license file from a TFTP server to the internal flash on the CP module:

```
VSP-9012:1(config)# copy 192.0.2.20:license.lic /intflash/
license.dat
```

Load the license:

```
VSP-9012:1(config)# load-license
```

Variable definitions

Use the data in the following table to help you install a license with the `copy` command.

Table 51: Variable definitions

Variable	Value
<a.b.c.d>	Specifies the IPv4 address of the TFTP server from which to copy the license file.
<x:x:x:x:x:x:x:x>	Specifies the IPv6 address of the TFTP server from which to copy the licence file. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
<destfile>	Specifies the name of the license file when copied to the flash. The destination file name must be lower case and have a file extension of .dat. For example, license.dat.
<srcfile>	Specifies the name of the license file on the TFTP server. For example, license.lic or license.dat. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Showing a license file

About this task

Display the existing software licenses on your device.

Procedure

Show the existing software licenses on your device:

```
show license
```

Example

```
VSP-9012:1>show license

        License file name      :    /intflash/premiersitelicense.dat
        License Type           :    PREMIER
        MD5 of Key             :    67d9b8d4 e58172cf 91a3a4c2 5f03c00a
        MD5 of File            :    185f5e5c fea563d0 dd1a777c 8d54208c
        Generation Time        :    2010/04/12 11:18:08
        Expiration Time        :
        Base Mac Addr          :    00:24:7f:9f:60:00
        flags                  :    0x00000001 SINGLE
        memo                   :
```

Chapter 18: License installation using EDM

Install and manage a license file for Avaya Virtual Services Platform 9000 by using Enterprise Device Manager (EDM).

Installing a license file

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 9000 on which you need to install the license. Otherwise, the system does not unblock the licensed features.
- If the chassis uses two CP modules, you do not need to install the license file on the secondary CP module. After you enable High Availability, the primary CP module copies the license vectors to the secondary CP module during table sync and the trial period countdown stops. This action ensures that the run time vectors of the primary and secondary CP module are the same. After you save the configuration on the primary CP module, the system copies the license file to the secondary CP module.

  In warm-standby mode, the system does not synchronize the license vectors with the secondary CP module. However, the system copies the license file to the secondary CP module after you save the configuration using the saveRuntimeConfigtoSlave option.

About this task

Install a license file on Avaya Virtual Services Platform 9000 to enable licensed features.

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

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 flash device and the name of the license file.

   The license file name must be lower case and have a file extension of .dat.
6. Select **start**.

7. Click **Apply**.

   The license file is copied to the flash of the primary CP module. 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. If the chassis uses two CP modules, you need to save the configuration so that the license file is copied to the secondary CP module. 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 cancels the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory

Name	Description
	• outOfSpace • fileNotFound

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.
VirtualIpAddr	Configures the virtual IP address that is advertised by the primary CPU and stored in the switch configuration file.
VirtualNetMask	Configures the net mask of the virtual management IP address.
VirtualIpv6Address	Configures the virtual IPv6 address that is advertised by the primary CPU. and stored in the switch configuration file.
VirtualIPv6Prefix Length	Configures the length of the virtual IPv6 prefix entry.
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.
LastRunTimeConfigSaveToSlave	Displays the last run-time configuration saved to the standby device.

Name	Description
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: • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration • saveRuntimeConfigToSlave—saves the current run-time configuration to the standby CPU • loadLicense—loads a software license file to enable features
ActionGroup2	Can be following action: • resetIstStatCounters—resets the IST statistic counters
ActionGroup3	Can be the following action: • flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be one of the following actions: • softReset—resets the device without running power-on tests • cpuSwitchOver—switch control from one CPU to another
Result	Displays a message after you click **Apply**.

Chapter 19: 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 9000, 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 9000 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.

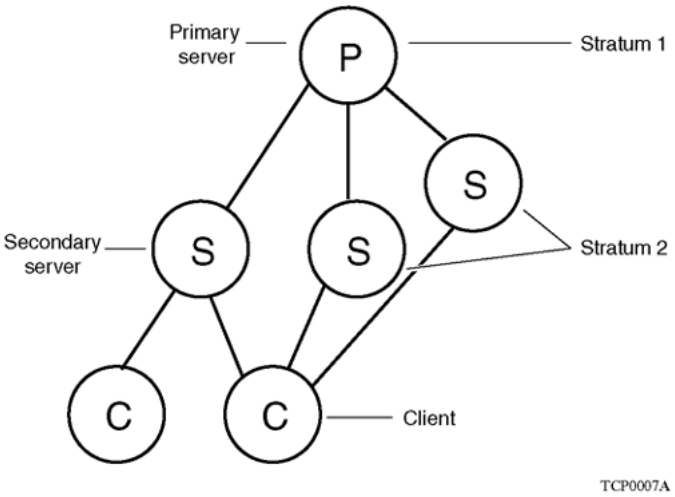

Figure 3: NTP time servers forming a synchronization subnet

In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary (master-backup) 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 3: NTP time servers forming a synchronization subnet on page 176. 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 9000 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 4: NTP time servers operating in unicast client mode on page 178. 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.

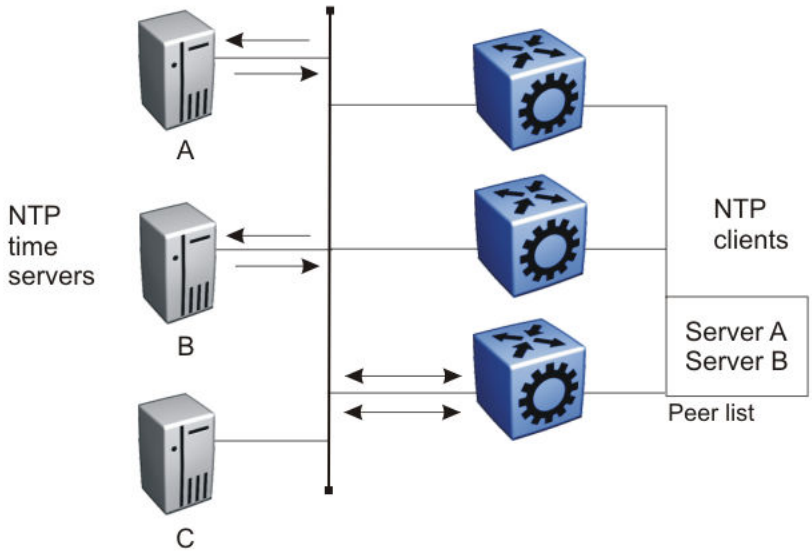

Figure 4: NTP time servers operating in unicast client mode

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 9000 uses the Message Digest 5 (MD5) 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. The MD5 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 20: 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 9000 and ensure that the NTP server is reachable through this interface. For instructions, see *Avaya Virtual Services Platform 9000 Configuration — IP Routing*, NN46250–505.
- Ensure the Real Time Clock is present on the CP module.

Important:

NTP server MD5 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.

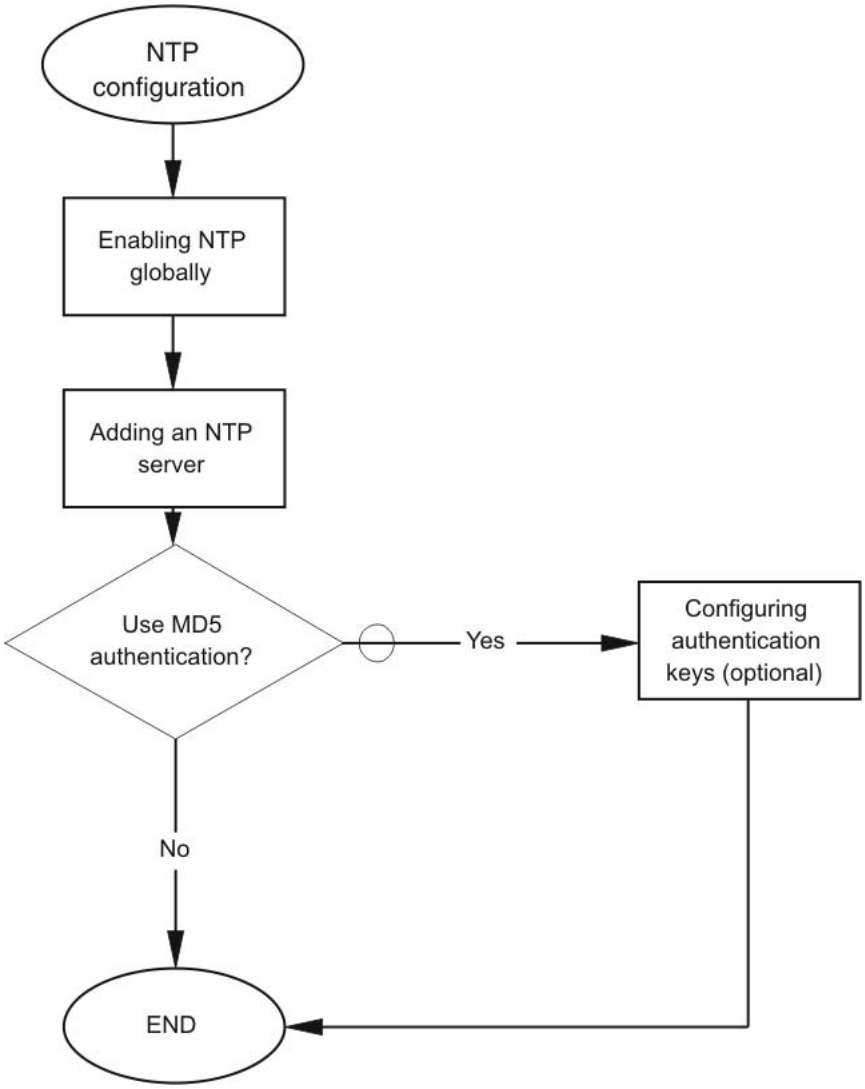

Figure 5: NTP configuration procedures

Enabling NTP globally

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Enable NTP globally. Default values are in effect for most parameters. You can customize NTP by modifying parameters.

Procedure

1. Enable NTP globally:
   ```
   ntp interval <10-1440>
   ```
2. Create an authentication key:
   ```
   ntp authentication-key <1-2147483647> WORD<0-8>
   ```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Enable the Network Time Protocol globally and specify the time, in minutes, between successive NTP updates:

```
VSP-9012:1(config)#ntp interval 10
```

Variable definitions

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

Table 52: Variable definitions

Variable	Value
authentication-key <1-2147483647> WORD<0–8>	Creates an authentication key for MD5 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. *WORD<0–8>* specifies the secret key.
interval <*10-1440*>	Specifies the time interval, in minutes, between successive NTP updates. • interval is expressed as an integer in a range from 10–1440 The default value is 15. To set this option to the default value, use the default operator with the command. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

Adding an NTP server

Before you begin

- You must log on to Global Configuration mode in ACLI.

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

1. Add an NTP server:
   ```
   ntp server <A.B.C.D>
   ```
2. Configure additional options for the NTP server:
   ```
   ntp server <A.B.C.D> [auth-enable] [authentication-key
   <0-2147483647>]
   ```
3. Activate the NTP server:
   ```
   ntp server <A.B.C.D> enable
   ```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# ntp server 192.0.2.187
```

Variable definitions

Use the data in the following table to use the `ntp server` command.

Table 53: Variable definitions

Variable	Value
A.B.C.D	Specifies the IP address of the server.
auth-enable	Activates MD5 authentication on this NTP server. The default is no MD5 authentication. To set this option to the default value, use the default operator with the command.

Variable	Value
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 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.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.

Configuring authentication keys

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Configure NTP authentication keys to use MD5 authentication.

Procedure

1. Create an authentication key:
   `ntp authentication-key <1-2147483647> WORD<0-8>`
2. Enable MD5 authentication for the server:
   `ntp server <A.B.C.D> auth-enable`
3. Assign an authentication key to the server:
   `ntp server <A.B.C.D> authentication-key <0-2147483647>`

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
```

Create the authentication key:

```
VSP-9012:1(config)# ntp authentication-key 5 test
```

Enable MD5 authentication for the NTP server:

```
VSP-9012:1(config)# ntp server 192.0.2.187 auth-enable
```

Variable definitions

Use the data in the following table to use the `ntp` and `ntp server` commands.

Table 54: Variable definitions

Variable	Value
A.B.C.D	Specifies the IP address of the server.
auth-enable	Activates MD5 authentication on this NTP server. The default is no MD5 authentication. To set this option to the default value, use the default operator with the command.
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 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.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.

Chapter 21: 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 9000 and ensure that the NTP server is reachable through this interface. For instructions, see *Avaya Virtual Services Platform 9000 Configuration — IP Routing*, NN46250–505.
- Ensure the Real Time Clock is present on the CP module.

Important:

NTP server MD5 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 basic elements of IP multicast routing.

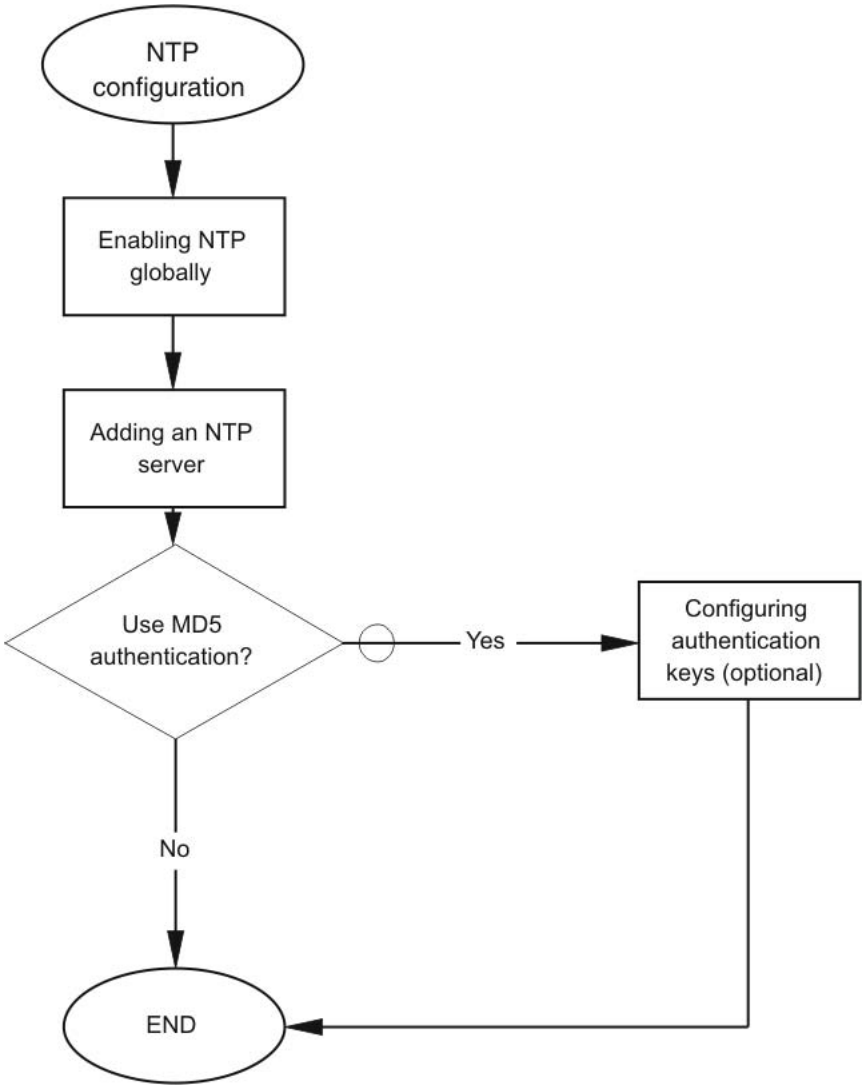

Figure 6: NTP configuration procedures

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	Specifies the time interval (10–1440 minutes) between successive NTP updates. The default interval is 15 minutes. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then reenable it.

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 authentication on this NTP server. MD5 produces a message digest of the key. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The default is no MD5 authentication.
KeyId	Specifies the key ID used to generate the MD5 digest for this NTP server. You must specify a number between 1–214743647. The default is 0, which indicates that authentication is disabled.
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 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.
6. 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 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 key that generates the MD5 digest. You must specify an alphanumeric string between 0–8 **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 #.

Chapter 22: Secure Shell fundamentals

Secure Shell (SSH) is a client and server protocol that specifies the way to conduct secure communications over a network. Secure CoPy (SCP) is a secure file transfer protocol. SCP is off by default, but you turn it on when you enable SSH using the **`config bootconfig flags`** command. 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 CoPy 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.

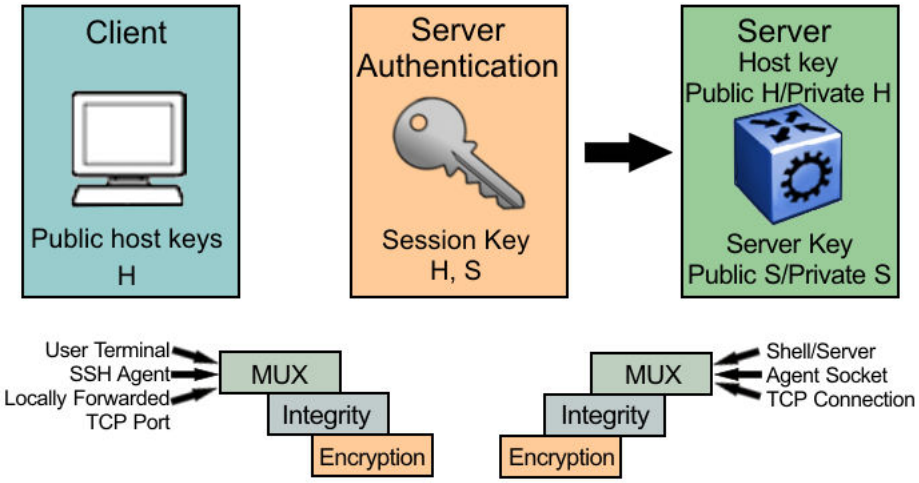

Figure 7: Overview of the SSH protocol

By using a combination of host, server, and session keys, the SSH 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 Virtual Services Platform 9000, you can use the SSH client to make a secure connection to Virtual Services Platform 9000 and work with commercially available SSH clients. For more information about supported clients, see Table 56: Third-party SSH and SCP client software on page 197. VSP 9000 also supports outbound connections to the remote SSH servers to provide complete inbound and outbound secure access.

Security features

The SSH protocol supports the following security features:

- Authentication. This feature determines, in a reliable way, the SSH client. During the log on process, the SSH client is queried for a digital proof of identity.

  Supported authentications are RSA (SSH-1), DSA (SSH-2), and passwords (both SSH-1 and SSH-2).

- Encryption. The SSH 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, and AES256-cbc

- 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 SSH server detects this alteration.

Downloading and enabling security encryption

Important:

Due to export restrictions, the encryption capability is separate from the main image. For more information about how to download and enable security encryption, see Downloading the software on page 201. For more information about how to enable the SSH server through ACLI, see Enabling the SSH server on page 202. The SSH server does not function properly without the use of this image.

SSH considerations using EDM

You must use the ACLI to initially configure SSH. You can use Enterprise Device Manager (EDM) to change the SSH configuration parameters. However, Avaya recommends that you use ACLI. Avaya also recommends that you use the console port to configure the SSH parameters.

Important:

Do not enable SSH secure mode using Enterprise Device Manager (EDM). If you enable secure mode, then the system disables Simple Network Management Protocol (SNMP). This locks you out of the EDM session. Enable SSH secure mode using ACLI.

When you enable SSH, the system disables SNMPv1, SNMPv2 and SNMPv3. You can disable block-snmp and re-enable SNMPv3 after you enable SSH. However, if you enable SSH, then the system disables EDM and you cannot re-enable EDM at the same time the system enables SSH.

SSH support for IPv6

On IPv6 networks, VSP 9000 supports SSH server only. VSP 9000 does not support outbound SSH client over IPv6. On IPv4 networks, VSP 9000 supports both SSH server and SSH client.

Interoperability

The VSP SSH client can operate with the following SSH servers:

- another VSP 9000
- ERS 8600/8800
- Linux running Open SSH

Outbound connections

The SSH client supports SSH v2, DSA public key authentication and password authentication.

The SSH client is a secure replacement for outbound Telnet. Password authentication is the easiest way to use the SSH client feature. With VSP 9000, you can use the SSH client feature as shown in the following example:

Linux/PC ssh (password) > **VSP ssh (password)** > **VSP ssh (password)** > **VSP**

Instead of password authentication, you can use DSA public key authentication between the VSP SSH client and the SSH server. Before you can perform a public key authentication, you must generate the key pair files and distribute the key files to all the SSH client and 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. The following is an example of DSA public key authentication between the VSP SSH client and the SSH server:

Linux/PC ssh (DSA authorization) > **VSP ssh (DSA authorization)** > **VSP ssh (DSA authorization)** > **VSP**

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 SSH client automatically prompts you for password authentication. If the SSH client succeeds with the authentication, then a new secured SSH session is established to the remote SSH server.

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 SSH server.

SSH version 2

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 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 SSH-2 protocol.

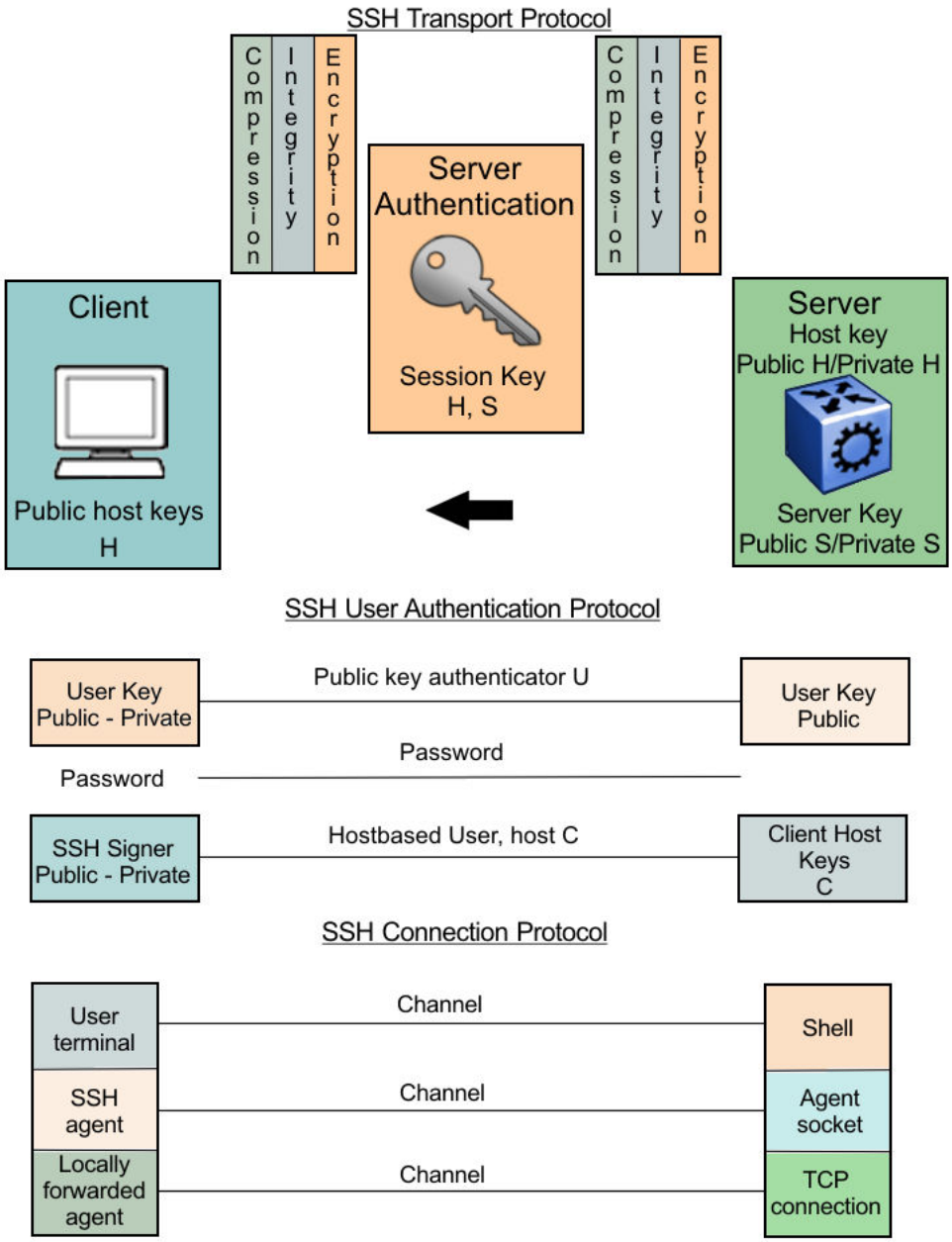

Figure 8: Separate SSH version 2 protocols

The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

Important:

The SSH-1 and SSH-2 protocols are not compatible. While the SSH implementation in Virtual Services Platform 9000 supports both versions of SSH, Avaya recommends that you use the more secure version, the SSH-2 protocol.

User ID log of an SSH session established by SCP client

Virtual Services Platform 9000 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:

```
CPU5 [01/02/03 03:28:04] SSH INFO SSH: User rwa login /pty/sshd1 from 198.202.188.178
```

- `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.

SSH password authentication uses the same login and password authentication mechanism as Telnet. SSH v2 client also supports DSA public key authentication compatible with VSP 9000 SSH server and Linux SSH server for SSH v2.

If VSP 9000 is the client, use the following table to locate the DSA user key files for DSA authentication for user access level `rwa`.

Table 55: DSA user key files

SSH server	SSH client side	SSH server side
VSP 9000	/intflash/.ssh/id_dsa_rwa (private key) /intflash/.ssh/id_dsa_rwa.pub (public key)	/intflash/.ssh/dsa_key_rwa (public key)
Linux with Open SSH	~/.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)

Important:

Before performing the DSA authentication, you must copy the public key file on the server side from the client side public key file.

After you attempt to make an SSH connection, the client looks in the internal flash on the local VSP 9000 for the public key pair files. If the key files exist, the SSH client prompts you for the password to decrypt the key files. If the password is correct, the SSH client initiates the DSA key authentication with the remote SSH server. The client looks for the login user access level public key file to process and validate the public key authentication. If the DSA authentication is successful, then the SSH session is established.

If there is no matching user key pair files, or if the DSA authentication fails, you are prompted for a password to attempt password authentication automatically.

If the remote SSH server is a Linux system which is based on Open SSH implementation, the server looks for the login user public key file ~/.ssh/authorized_keys by default for DSA authentication. For Linux SSH

client, the user DSA key pair files are located in the user home directory as ~/.ssa/id_dsa and ~/.ssa/id_dsa.pub.

Block SNMP

The boot flag setting for block-snmp (**boot config flags block-snmp**) and the runtime configuration of SSH secure (**ssh secure**) each modify the block-snmp boot flag. If you enable SSH secure mode, the system automatically sets the block-snmp boot flag to true; the change takes effect immediately. After enabling SSH in secure mode, you can manually change the block-snmp flag to false to allow both SSH and SNMP access.

Important:

The block flag setting for block-snmp blocks Simple Network Management Protocol (SNMP)v1, SNMPv2, and SNMPv3.

SSHv1 clients

If SSHv1 clients (both Unix and PC) are connected to the device and SSH is disabled, the following error message appears before the logoff message:

```
VSP-9012:5# [09/24/09 13:41:16] ERROR Task=sshdSession Write failed:
S_iosLib_INVALID_FILE_DESCRIPTOR
```

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.

Third-party SSH and SCP client software

The following table describes the third-party SSH and SCP client software that has been tested but is not included with this release.

Table 56: Third-party SSH and SCP client software

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
Tera Term Pro with TTSSH extension MS Windows	• Supports SSH-1 and SSH-2. • Authentication: - RSA - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys.	• Client distribution does not include SCP client.
Secure Shell Client Windows 2000	• Supports SSH-2 client. • Authentication - DSA - Password	• Client distribution includes an SCP client that is not compatible with Virtual Services Platform 9000.

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
	• Provides a keygen tool. • It creates a DSA key in SSHv2 format. • Virtual Services Platform 9000 generates a log message stating that a DSA key has been generated.	
OpenSSH Unix Solaris 2.5 / 2.6	• Supports SSH-1 and SSH-2 clients. • Authentication: - RSA - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys in SSH v1 format.	• Client distribution includes an SCP client that is supported on Virtual Services Platform 9000.

After you install one of the SSH clients you must generate a client and server key using the RSA or DSA algorithms

Important:

Authentication keys are not saved to the secondary CP module, if one is present. Use TFTP or FTP to copy the keys to the secondary CP module.

Virtual Services Platform 9000 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_pub.key

If a DSA key pair does not exist, then Virtual Services Platform 9000 automatically generates one when you enable the SSH server. To authenticate a client using DSA, the administrator must copy the public part of the client DSA key to Virtual Services Platform 9000.

DSA authentication access level and file name

The following table lists the access levels and file names you can use to store the SSH client authentication information using DSA.

Table 57: DSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in IETF format (SSHv2)	RWA	/intflash/.ssh/dsa_key_rwa_ietf
	RW	/intflash/.ssh/dsa_key_rw_ietf
	RO	/intflash/.ssh/dsa_key_ro_ietf

Client key format or WSM	Access level	File name
	L3	/intflash/.ssh/dsa_key_rwl3_ietf
	L2	/intflash/.ssh/dsa_key_rwl2_ietf
	L1	/intflash/.ssh/dsa_key_rwl1_ietf
Client key in non IETF format	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

Virtual Services Platform 9000 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 9000 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 9000.

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 58: RSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in IETF format	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

SSL certificates

Virtual Services Platform 9000 loads the SSL certificate during the system boot-up time. If a certificate exists in the `/intflash/.ssh/` directory during the boot-up process, then the system loads that certificate. 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/.ssh/` directory, and then rename the files to host.cert and host.key. Reboot the system and the new certificate will be loaded during the boot-up process.

The system does not validate the expiration date on the certificate and performs no action after the certificate expires. You can either replace the host.cert and host.key files with new files (if the certificate

is a user generated certificate), or delete the host.cert and host.key files, and then reboot the system to load a new certificate after the original certificate expires.

Chapter 23: Secure Shell configuration using ACLI

Use Secure Shell (SSH) to enable secure communications support over a network for authentication, encryption, and network Integrity.

On IPv6 networks, VSP 9000 supports SSH server only. VSP 9000 does not support outbound SSH client over IPv6. On IPv4 networks, VSP 9000 supports both SSH server and SSH client.

Before you begin

- Disable the sshd daemon. All SSH 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 49.
- Avaya recommends that you use the console port to configure the SSH parameters.

Downloading the software

Download new software to upgrade the Avaya Virtual Services Platform 9000. 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: www.avaya.com/support. 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 and you can enable them when the file is stored on flash.

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 *Avaya Virtual Services Platform 9000 Release Notes*, NN46250–401.

Important:

You must load the security encryption modules on the device before you can use the protocol.

Procedure

1. From an Internet browser, browse to www.avaya.com/support.
2. Click **DOWNLOADS & DOCUMENTS**.
3. In the product search field, type **Virtual Services Platform 9000**.
4. In the **Choose Release** field, click a release number.
5. Select **Downloads**.
6. Click **ENTER**.
7. Click the download title to view the selected information.
8. Click the file you want to download.
9. Login to download the required software file.
10. Use an FTP client in binary mode to transfer the file to the Virtual Services Platform 9000, or transfer it using an external USB device.

Enabling the SSH server

Before you begin

- Download the file containing the SSH encryption software.

  Important:

  Due to export restrictions, the SSH encryption capability is separate from the main image. You must download the security encryption images to flash before you can load the encryption module. The SSH server does not function properly without the use of this image.

- You must log on to Global Configuration mode in ACLI.

About this task

Enable the SSH server to provide secure communications for accessing the switch.

Procedure

1. Enable the SSH server:
   ```
   boot config flags sshd
   ```
2. Save the configuration file:
   ```
   save config
   ```
3. Load the security encryption image:
   ```
   load-encryption-module {3DES|AES|DES}
   ```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Enable the SSH server:

```
VSP-9012:1(config)#boot config flags sshd
```

Save the boot cfg file:

```
VSP-9012:1(config)#save config
```

Load the Advanced Encryption Standard security encryption image:

```
VSP-9012:1(config)#load-encryption-module AES
```

Variable definitions

Use the data in the following table to use the `load-encryption-module` command.

Table 59: Variable definitions

Variable	Value
3DES	Loads the 3DES SSH encryption module.
AES	Loads the AES SSH encryption module.
DES	Loads the DES SSH encryption module.

Setting SSH configuration parameters

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Configure Secure Shell (SSH) parameters to support public and private key encryption connections.

Procedure

1. Enable DSA authentication:
   ```
   ssh dsa-auth
   ```
2. Generate a new DSA host key:
   ```
   ssh dsa-host-key [<512-1024>]
   ```
3. Generate a new SSH DSA user key:
   ```
   ssh dsa-user-key <rwa | rw | ro | rwl1 | rwl2 | rwl3 >
   ```
4. Configure the maximum number of SSH sessions:
   ```
   ssh max-sessions <0-8>
   ```
5. Enable password authentication:
   ```
   ssh pass-auth
   ```
6. Configure the SSH connection port:
   ```
   ssh port <1-65535>
   ```
7. Enable RSA authentication:
   ```
   ssh rsa-auth
   ```
8. Generate a new RSA host key:
   ```
   ssh rsa-host-key [<512-1024>]
   ```
9. Enable SSH secure mode:
   ```
   ssh secure
   ```
10. Configure the authentication timeout:
    ```
    ssh timeout <1-120>
    ```
11. Configure the SSH version:

```
ssh version <v2only|both>
```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Enable DSA authentication:

```
VSP-9012:1(config)#ssh dsa-auth
```

Configure the maximum number of SSH sessions:

```
VSP-9012:1(config)#ssh max-sessions 5
```

Variable definitions

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

Table 60: Variable definitions

Variable	Value
dsa-auth	Enables or disables the DSA authentication. The default is enabled. Use the no operator before this parameter, `no ssh dsa-auth`, to disable DSA authentication.
dsa-host-key [<512-1024>]	Generates a new SSH DSA host key. Specify an optional key size between 512 and 1024. The default is 1024. Use the no operator before this parameter, `no ssh dsa-host-key`, to disable SSH DSA host key.
dsa-user-key WORD <1–15><rwa | rw | ro | rwl1 | rwl2 | rwl3 >	Generates a new SSH DSA user key. WORD<1–15> specifies the user access level. The valid user access levels for Virtual Services Platform 9000 are: • 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. • rwl3 — Specifies read-write for Layer 3. Use the no operator before this parameter, `no ssh dsa-user-key <rwa|rw|rw|rwl1|rwl2|rwl3>`, to disable SSH DSA user key.
max-sessions <0-8>	Specifies the maximum number of SSH sessions allowed. A value from 0 to 8. Default is 4.

Variable	Value
pass-auth	Enables password authentication. The default is enabled.
port <1-65535>	Configures the SSH connection port. *<1-65535>* is the port number. The default is 22. **Important:** You cannot configure the following TCP ports as SSH connection ports: Ports 0 to 1024 (except port 22),1100, 4095, 5000, 5111, 6000, or 999.
rsa-auth	Enables RSA authentication. The default is enabled. Use the no operator before this parameter, `no ssh rsa-auth`, to disable RSA authentication.
rsa-host-key [<512-1024>]	Generates a new SSH RSA host key. Specify an optional key size between 512 and 1024. The default is 1024. Use the no operator before this parameter, `no ssh rsa-host-key`, to disable SSH RSA host key.
secure	Enables SSH in secure mode and immediately disables the access services SNMP, FTP, TFTP, rlogin, and Telnet. The default is disabled. Use the no operator before this parameter, `no ssh secure`, to disable SSH in secure mode.
timeout <1-120>	Specifies the SSH connection authentication timeout in seconds. Default is 60 seconds.
version <v2only|both>	Configures the SSH version. Default is v2only. **Important:** Avaya recommends setting the version to v2 only.

Verifying and displaying SSH configuration information

About this task

Verify that SSH services are enabled on Avaya Virtual Services Platform 9000 and display SSH configuration information to ensure that the SSH parameters are properly configured.

Procedure

Verify that SSH services are enabled and view the SSH configuration:

```
show ssh <global|session>
```

Example

Display global system SSH information:

```
VSP-9012:1>show ssh global

Total Active Sessions  : 0
        version            : v2only
        port               : 22
        max-sessions       : 4
        timeout            : 60
        action rsa-keygen  : rsa-keysize 1024
        action dsa-keygen  : dsa-keysize 1024
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : true
```

Variable definitions

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

Table 61: 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

Before you begin

- Download the file containing the SSH encryption software.

  Important:

  Due to export restrictions, the SSH encryption capability is separate from the main image. You must download the security encryption images to flash before you can load the encryption module. The SSH server does not function properly without the use of this image.

- You must log on to Privileged EXEC mode in ACLI.
- You must enable the SSH 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. Configure the SSH parameters to connect to a remote host.

On IPv6 networks, VSP 9000 supports SSH server only. VSP 9000 does not support outbound SSH client over IPv6. On IPv4 networks, VSP 9000 supports both SSH server and SSH client.

Procedure

Connect to a remote host:

```
ssh WORD<1-256> -l WORD<1-32> [-p <1-32768>]
```

Example

```
VSP-9012:1>enable

VSP-9012:1#ssh 192.0.2.1 -l rwa
```

Variable definitions

Use the data in the following table to use the `load-encryption-module` command.

Table 62: Variable definitions

Variable	Value
3DES	Loads the 3DES SSH encryption module.
AES	Loads the AES SSH encryption module.
DES	Loads the DES SSH encryption module.

Use the following table to use the `ssh` command.

Table 63: Variable definitions

Variable	Value
WORD<1-256>	Specifies the host name or IP address. On IPv6 networks, VSP 9000 supports SSH server only. VSP 9000 does not support outbound SSH client over IPv6. On IPv4 networks, VSP 9000 supports both SSH server and SSH client.
WORD<1–32>	Specifies the user login name of the remote SSH server.

Variable	Value
-p <1-32768>	Specifies the port number to connect to the remote SSH server. The default is 22.

Generating user key files

Before you begin

- Download the file containing the SSH encryption software.

  Important:

  Due to export restrictions, the SSH encryption capability is separate from the main image. You must download the security encryption image to flash before you can load the encryption module. The SSH server does not function properly without the use of this image.
- You must log on to Global Configuration mode in ACLI.
- You must enable the SSH server.

About this task

Configure the SSH parameters to generate DSA user key files.

Procedure

1. Create the DSA user key file:
   `ssh dsa-user-key [WORD<1-15>][size <512-4096>]`
2. Enter the encryption password to protect the key file.
3. Copy the user public key file to the remote SSH servers.
4. 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 Virtual Services Platform 9000 SSH client.

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

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:

```
VSP-9012:1(config)#ssh dsa-user-key rwa size 512
```

Variable definitions

Use the following table to use the `ssh dsa-user-key` command.

Table 64: Variable definitions

Variable	Value
WORD<1–15 >	Specifies the user access level. The valid user access levels for Virtual Services Platform 9000 are: • `rwa`—Specifies read-write-all. • `rw`—Specifies read-write. • `ro`—Specifies read-only • `rwl3`—Specifies read-write for Layer 3. • `rwl2`—Specifies rread-write for Layer 2. • `rwl1`—Specifies read-write for Layer 1.
size*<512–4096>*	Specifies the size of the DSA user key. The default is 1024 bits.

Chapter 24: Secure Shell configuration using Enterprise Device Manager

Use Secure Shell (SSH) to enable secure communications support over a network for authentication, encryption, and network Integrity.

On IPv6 networks, VSP 9000 supports SSH server only. VSP 9000 does not support outbound SSH client over IPv6. On IPv4 networks, VSP 9000 supports both SSH server and SSH client.

For more information, see Changing Secure Shell configuration parameters on page 212.

For information about downloading and enabling security encryption, see Downloading the software on page 201.

Downloading the software

Download new software to upgrade the Avaya Virtual Services Platform 9000. 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: www.avaya.com/support. 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 and you can enable them when the file is stored on flash.

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 *Avaya Virtual Services Platform 9000 Release Notes*, NN46250–401.

Important:

You must load the security encryption modules on the device before you can use the protocol.

Procedure

1. From an Internet browser, browse to www.avaya.com/support.
2. Click **DOWNLOADS & DOCUMENTS**.
3. In the product search field, type **Virtual Services Platform 9000**.
4. In the **Choose Release** field, click a release number.
5. Select **Downloads**.
6. Click **ENTER**.
7. Click the download title to view the selected information.
8. Click the file you want to download.
9. Login to download the required software file.
10. Use an FTP client in binary mode to transfer the file to the Virtual Services Platform 9000, or transfer it using an external USB device.

Changing Secure Shell configuration parameters

Before you begin

- The user access level is read/write/all community strings.

About this task

You can use Enterprise Device Manager to change the SSH configuration parameters. However, Avaya recommends using the ACLI to perform the initial configuration of SSH.

If the SSH service is enabled, all fields are dimmed until the SSH service is disabled. You must disable the SSH service before setting the SSH 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. Click **Apply**.

SSH field descriptions

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

Name	Description
Enable	Enables, disables, or securely enables SSH. The options are: • false • true • secure Select false to disable SSH services. Select true to enable SSH services. Select secure to enable SSH and disable access services (SNMP, FTP, TFTP, rlogin, and Telnet). The default is false. **Important:** 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.
Version	Configures the SSH version. The options are: • v2only • both Set to both or v2only. The default is v2only.
Port	Configures the SSH connection port number. The default is 22.

Name	Description
	Important: You cannot configure the following TCP ports as SSH connection ports: Ports 0–1024 (except port 22),1100, 4095, 5000, 5111, 6000, or 999.
MaxSession	Configures the maximum number of SSH sessions allowed. The value can be from 0–8. The default is 4.
Timeout	Configures the SSH authentication connection timeout in seconds. The default is 60 seconds.
KeyAction	Configures the SSH key action. The options are: • none • generateDsa • generateRsa • deleteDsa • deleteRsa
RsaKeySize	Configures SSH RSA key size. The value can be from 512–1024. The default is 1024.
DsaKeySize	Configures the SSH DSA key size. The value can be from 512–1024. The default is 1024.
RsaAuth	Enables or disables SSH RSA authentication. The default is enabled.
DsaAuth	Enables or disables SSH DSA authentication. The default is enabled.
PassAuth	Enables or disables SSH RSA password authentication. The default is enabled.

Chapter 25: System access fundamentals

This section contains conceptual information about how to access Avaya Virtual Services Platform 9000 and create users and user passwords for access.

Logging on to the system

After the startup sequence is complete, the login prompt appears. The following table shows the default values for login and password for the console and Telnet sessions.

Table 65: 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
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	rwa	rwa

Access level	Description	Default logon	Default password
	allows you to change the Avaya command line interface (ACLI) and Web-based management user names and passwords and the SNMP community strings.		

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.
```

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.

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 9000 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 *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

Managing the system using different VRF contexts

You can use Enterprise Device Manager (EDM) to manage the system using different virtual router forwarding (VRF) contexts. If you connect to the system using EDM in the GlobalRouter (VRF 0) context, then you can manage the entire system. If you connect to the system using EDM in a different VRF context, then you have limited capability to manage the system. For example, you can manage only the ports assigned to this VRF. In addition, many of the EDM management functions are not available to you. You can manage only those functions and components assigned to that specific VRF.

Virtual Services Platform 9000 provides the MgmtRouter VRF by default. Use this VRF to configure the management port for out-of-band (OOB) management. You cannot delete this VRF.

Specify the VRF instance name on the EDM logon page before you log on to the system.

With the use of user names and context names (SNMPv3), and community strings (SNMPv1/v2) , you can assign different VRFs to manage selected components, such as ports and VLANs. For more information about context names and community strings, see *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

ACLI passwords

The switch ships with default passwords set for access to ACLI 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 master central processing unit (CPU) in three consecutive instances, then the CPU locks for 60 seconds.

Virtual Services Platform 9000 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 9000, 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 9000 (ro, l1, l2, l3, rw, rwa)
- Command access (single instance)–indicates whether the user has access to the commands on the RADIUS server
- ACLI 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 (SSH), and remote login (rlogin). You can enable or disable access services by configuring flags.

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 and IPv6 with no difference in configuration or functionality.

Web interface passwords

Virtual Services Platform 9000 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 *Avaya Virtual Services Platform User Interface Fundamentals*, NN46250–103.

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 *Avaya Virtual Services Platform 9000 Quick Start*, NN46250–102.

Password encryption

Virtual Services Platform 9000 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.

Chapter 26: 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

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

Enable an access level:

```
password access-level WORD<2-8>
```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Block ACLI access to Layer 1 to control the configuration actions of various users:

```
VSP-9012:1(config)#no password access-level l1
```

Variable definitions

Use the data in the following table to use the `password access-level` command.

Table 66: Variable definitions

Variable	Value
WORD<2–8>	Permits or blocks this access level. The available access level values are as follows: • 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. 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.

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.
- You must log on to Global Configuration mode in ACLI.

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 9000, 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.

In hsecure mode, the master Control Processor (CP) module synchronizes the password aging time with the secondary CP module. After the password expires, you must change the password in the master CP module to log on to the secondary CP module.

Procedure

1. Change a password:

   ```
   cli password WORD<1-20> {layer1|layer2|layer3|read-only|
   read-write|read-write-all}
   ```

2. Enter the old password.
3. Enter the new password.
4. Enter the new password a second time.
5. 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-9012:1>enable

VSP-9012:1#configure terminal
```

Change a password:

```
VSP-9012:1(config)#cli password smith read-write-all
```

Enter the old password:

```
VSP-9012:1(config)#winter
```

Enter the new password:

```
VSP-9012:1(config)#summer
```

Enter the new password a second time:

```
VSP-9012:1(config)#summer
```

Set password to an access level of read-write-all and the expiration period for the password to 60 days:

```
VSP-9012:1(config)#password access-level rwa aging-time 60
```

Variable definitions

Use the data in the following table to use the `cli password` command.

Table 67: 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 68: Variable definitions

Variable	Value
access level WORD<2–8>	Permits or blocks this access level. The available access level values are as follows: • 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. • *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

Before you begin

- You must log on to Global Configuration mode in ACLI.

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.

Virtual Services Platform 9000 supports access-policies over IPv4 and IPv6 with no difference to functionality or configuration.

Procedure

1. Create an access policy by assigning it a number:
   ```
   access-policy <1-65535>
   ```
2. Restrict the access to a specific level:
   ```
   access-policy <1-65535> access-strict
   ```
3. Configure access for an access policy:
   ```
   access-policy <1-65535> accesslevel <ro|rwa|rw>
   ```
4. 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>]
   ```
5. Configure optional access protocols for an access policy:
   ```
   access-policy <1-65535> [ftp] [http] [ssh] [telnet] [tftp]
   ```
6. Configure optional trusted username access for an access policy:
   ```
   access-policy <1-65535> host WORD<0-46> [username WORD<0-30>]
   ```
7. 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]
   ```
8. Enable the access policy:
   ```
   access-policy <1-65535> enable
   ```

9. Enable access policies globally:
   `access-policy`

Example

Assuming no access policies exist, start with policy 3 and name the policy policy3:

```
VSP-9012:1(config)# access-policy 3 name policy3
```

Add read-write-all access level to policy 3:

```
VSP-9012:1(config)# access-policy 3 accesslevel rwa
```

Add the usm group group_example to policy 3:

```
VSP-9012:1# access-policy 3 snmp-group group_example usm
```

Enable access strict:

```
VSP-9012:1(config)# access-policy 3 access-strict
```

Enable policy 3:

```
VSP-9012:1(config)# access-policy 3 enable
```

Variable definitions

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

Table 69: Variable definitions

Variable	Value
access-strict	Restrains access to criteria specified in the access policy. • 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-

Variable	Value
	write (rw) access but not for the read-only (ro) access. Use the no operator to remove this configuration.
host *WORD<0–46>*	For remote login access, specifies the trusted host address as an IP address. The Virtual Services Platform 9000 supports access-policies over IPv4 and IPv6 with no difference to functionality or configuration. Use the no operator to remove this configuration.
http	Activates the HTTP for this access policy. Use the no operator to remove this configuration.
mode <*allow*|*deny*>	Specifies whether the designated network address is allowed access to the system through the specified access service. The default is allow.
network <A.B.C.D> <A.B.C.D>	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. Virtual Services Platform 9000 supports access-policies over IPv4 and IPv6 with no difference to functionality or configuration. Use the no operator to remove this configuration.
precedence <*1-128*>	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.
snmp-group *WORD<1–32>* <snmpv1|snmpv2c|usm>	Adds an SNMP version 3 group under the access policy. *WORD<1–32>* is the SNMP version 3 group name consisting of 1–32 characters. <snmpv1|snmpv2c|usm> is the security model; either snmpv1, snmpv2c, or usm. Use the no operator to remove this configuration.
snmpv3	Activates SNMP version 3 for the access policy. Use the no operator to remove this configuration.
ssh	Activates SSH for the access policy.

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 *WORD<0–30>*	Specifies the trusted host user name for remote login access.

Specifying a name for an access policy

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Assign a name to an existing access policy to uniquely identify the policy.

Procedure

Assign a name to the access policy:

```
access-policy <1-65535> name WORD<0-15>
```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Assign a name to an access policy:

```
VSP-9012:1(config)#access-policy 10 name useraccounts
```

Variable definitions

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

Table 70: Variable definitions

Variable	Value
name WORD<0–15>	Specifies a name expressed as a string from 0–15 characters.

Allowing a network access to the switch

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Specify the network to which you want to allow access.

Procedure

Specify the network:

```
access-policy <1-65535> [mode <allow|deny>] [network <A.B.C.D>
<A.B.C.D>]
```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal
```

Specify the network to which you want to allow access:

```
VSP-9012:1(config)#access-policy 5 mode allow network
fe80::221:5aff:fe68:c98d 64
```

Variable definitions

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

Table 71: Variable definitions

Variable	Value
mode <*allow*|*deny*>	Specifies whether a designated network address is allowed or denied access through the specified access service. The default is allow.

Variable	Value
network <A.B.C.D> <A.B.C.D>	The IPv4 address and subnet mask, or the IPv6 address and prefix-length permitted, or denied, access through the specified access service.

Configuring access policies by MAC address

Before you begin

- You must log on to Global Configuration mode in ACLI.

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. Add the MAC address and configure the action for the policy:
   ```
   access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>
   ```
2. Specify the action for a MAC address that does not match the policy:
   ```
   access-policy by-mac action <allow|deny>
   ```

Example

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
```

Add the MAC address:

```
VSP-9012:1(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 72: Variable definitions

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00>	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.

Chapter 27: 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.

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**.

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.

Name	Description
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.
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

Name	Description
	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.

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 Avaya Virtual Services Platform 9000, 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**.

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.

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.

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 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 and IPv6 addresses, with no difference in configuration or functionality.

On IPv6 networks, VSP 9000 supports SSH server, remote login (rlogin) server and Remote Shell (rsh) server only. VSP 9000 does not support outbound SSH client over IPv6, rlogin client over IPv6 or rsh client over IPv6. On IPv4 networks, VSP 9000 supports both server and client for SSH, rlogin and rsh.

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.
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 **NetInetAddrType**.
12. In the **NetInetAddress** box, type an IP address.
13. In the **NetInetAddrPrefixLen** box, type the prefix length.

14. In the **TrustedHostInet Address** 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	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.
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	Indicates the source network Internet address type as one of the following. • any • IPv4 • IPv6 IPv4 is expressed in the format a.b.c.d. IPv6 is expressed in the format x:x:x:x:x:x:x:x.
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. If the type is IPv6, you must enter an IPv6 address. You do not

Name	Description
	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. If the type is IPv6, you must enter an IPv6 address and prefix 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. **Important:** You cannot use wildcard entries in the TrustedHostInetAddr field. If the type is IPv4, you must enter an IPv4 address and mask length. If the type is IPv6, you must enter an IPv6 address and prefix length.
TrustedHostUserName	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. **Important:** 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.
AccessLevel	Specifies the access level of the trusted host as one of the following: • readOnly • readWrite • readWriteAll The default is readOnly.
Usage	Counts the number of times this access policy applies.
AccessStrict	Activates or disables strict access criteria for remote users.

Name	Description
	If selected, a user must use an access level identical to the one you selected in the dialog box to use this service. • selected: remote login users can use only the currently configured access level • cleared: remote users can use all access levels **Important:** 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. The default is false.

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 navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. Select the **EnableAccessPolicy** check box.
5. Click **Apply**.
6. Click **Close**.

Chapter 28: VSP Talk fundamentals

Use VSP Talk to remotely monitor your Virtual Services Platform 9000 on your computer or mobile device through an instant messaging (IM) client.

To communicate with the switch through VSP Talk you use the Instant Messaging Command Line Interface (IMCLI).

IMCLI is optimized for use with Instant Messaging and differs in behavior, capability, and characteristics from ACLI.

With VSP Talk, through IMCLI , you can query your switch about system and performance information. And the switch can send system information, performance, and alarm conditions to your smart phone or computer.

You must enable event-notification so that VSP Talk can send notifications about alarm conditions to your smart phone or computer.

The device or smart phone you use to connect to the switch must be equipped with IM client software through the IM service you use.

VSP Talk is included with the Base License.

Supported IM clients

Although VSP Talk supports several IM clients, you can use only one IM service at a time. If you try to enable a second IM client, then the software displays an error.

VSP Talk supports connectivity to the following IM servers:

- Goggle Talk
- Avaya Software Communication System IM Server

Note:

To connect to an Avaya Software Communication System IM server, you must install an officially-signed X.509 certificate on a Linux machine where the Software Communications System IM server runs in conjunction with the correct DNS SRV record. Or you can manually install the X.509 certificate on VSP 9000/intflash file system without an officially signed X.509 certificate.

VSP Talk supports the Extensible Messaging and Presence Protocol (XMPP), used by Google Talk and Avaya SCS IM Server.

XMPP is an open communications protocol, based on Extensible Markup Language (XML), used for real-time communication.

Getting started

You use VSP Talk to configure your switch as an IM client with an IM client account.

Then, through their IM client accounts, you configure individuals who monitor the device remotely as contacts of the switch

VSP Talk on the switch becomes an IM client that communicates with the administrators who need to monitor the switch.

To prepare to use VSP Talk, do the following:

1. Configure IP Domain Name Service before you configure VSP Talk.
2. Decide which IM service you want to use.
3. Create an IM client account for the switch through the IM service you selected.

   Tip:

   If you use Google Talk for IM, then you must use a Gmail account.
4. Create IM client accounts, through the IM service you selected, for each individual who needs to remotely monitor the device.

   Note:

   You can use existing IM client accounts, as long as they are with the IM service you plan to use for VSP Talk, but you must agree to the Terms of Service of the IM service provider when you create IM accounts for the switch and for individuals who remotely access the device.

To configure VSP Tallk, do the following:

1. On Virtual Services Platform 9000, using either ACLI or EDM, create the VSP Talk application.
2. Assign an endpoint address to VSP Talk that is in the same IP subnet as an existing VSP IP interface, either in-band or out-of-band.

   Do not use an existing VSP IP address, either in-band or out-of-band, as the VSP Talk endpoint address.

   Tip:

   Ensure that the endpoint address is separate from mission critical applications.
3. Define the VSP Talk IM client username, using the IM client account for the switch.
4. Define the VSP Talk IM client password, using the IM client account for the switch.
5. Because most networks require you to configure a proxy server to access the Internet, configure VSP Talk for the proxy server.
6. Add contacts (buddies in ACLI or group members in EDM) using the IM client accounts for the individuals who need to remotely monitor the device.

   After you become a group member or buddy with the switch, then communication to and from Virtual Services Platform 9000 can take place using IMCLI.
7. Enable VSP Talk.

Important:

Avaya recommends that you disable VSP Talk before you make a switch configuration change, then re-enable VSP Talk after the change is complete.

Detailed information about configuration and commands is available in the configuration chapters of this document.

Using VSP Talk

To start using VSP Talk, do the following.

1. After you configure VSP Talk on the switch, log in to your IM account.
2. Add the switch as a contact, using the IM client account address you configured for the device.
3. Start an IMCLI session with the IM contact that represents the device.

Supported commands on IMCLI

VSP Talk IMCLI is a unique instant messaging interface that differs in behavior and capability from ACLI. IMCLI is optimized for use in Instant Messaging.

IMCLI syntax and abbreviations:

The following table contains the examples of the full syntax and abbreviated syntax that you can use in IMCLI.

Because VSP Talk supports the use of abbreviations for commands through IMCLI you can use the first letter of each operator in a command to implement it on the device.

Full IMCLI command syntax	Abbreviated IMCLI command syntax	Description
show sys-info	ss	Displays system description, name, uptime, location, contact, card, power supply, and fan status.
show khi performance cpu slot#	skpc#	Displays CPU utilization per slot.
show khi performance memory slot#	skpm#	Displays memory utilization per slot.
show khi performance buffer-pool slot#	skbp#	Displays buffer pool utilization per slot.
show event-notification	se	Displays event-notification history.
enable event-notification	ee	Enables event notification.
disable event-notification	de	Disables event notification.

Full IMCLI command syntax	Abbreviated IMCLI command syntax	Description
help	h	Displays help; the system displays the same message for syntax errors.
Note: Slot # is a value from 1 to 12 and 21 to 26. A value of 1 is for CP card #1. A value of 2 is for CP card #2. Values between 3 and 12 are for IO cards 3 to 12. Values between 21 and 26 are for SF cards 1 to 6.		

VSP Talk event notification

Use event notification to receive status updates from the switch and to allow the switch to notify you about alarm conditions.

Event notification is enabled by default.

If you disable event notification you can re-enable event notifications in ACLI or EDM.

Tip:

In ACLI, use the command **`vsptalk event-notification enable`**.

When you enable event notification on VSP Talk, you can receive notification about the following items:

- High CPU utilization alarm
- IST Link status change
- Critical process termination
- Boot sequence successful log
- Login and logout activity
- Physical hardware changes

High Availability

VSP 9000 supports VSP Talk in High Availability (HA-CPU) mode.

The switch does not support runtime HA.

Platforms with two CPUs use HA-CPU mode to recover quickly from a failure of the master CPU.

Tip:

To leverage the advantages of HA for VSP Talk connected to an Avaya Software Communication System IM server (or some of the other privately-configured IM servers), you must install an X.509 certificate on both CPUs.

Limitations

Following are limitations associated with VSP Talk.

- Rate-limiting — Google servers use rate limiting of IM messages to limit the number of IM messages within a defined period of time. When VSP Talk and the IM client generate a large number of

messages to these servers, the servers discard messages without any indication. You must log out of the IM service and log in again to recover. And you may not be able to access the discarded messages when you log in again.

- Contacts — You can add a maximum of 12 contacts (buddies in ACLI or group members in EDM) who can communicate with the switch through VSP Talk.
- Commands — VSP Talk provides only a limited set of specific show commands and event notifications. VSP Talk does not provide read-write-all access, it is a monitoring tool only.
- IM Client — Simultaneous use of more than one IM service is not supported by VSP Talk. If you try to enable a second server, then the software displays an error.

Security

To insulate mission critical applications from value-added applications, VSP Talk is a separate process from the main routing and switching application.

As part of the VSP Talk process, when you configure the VSP Talk endpoint address you must assign an endpoint address to VSP Talk that is in the same IP subnet as an existing VSP IP interface, either in-band or out-of-band.

Do not use an existing VSP IP address, either in-band or out-of-band, as the VSP Talk endpoint address.

Ensure that the endpoint address is separate from mission critical applications.

Do not use an IP address already assigned to a port or VLAN on the device, and do not use the management IP address as the endpoint IP address for VSP Talk.

Messages sent between VSP Talk client and the Google or Avaya servers use Transport Layer Security (TLS) encryption.

Transport Layer Security Encryption (TLS) is enabled by default. You cannot change this configuration.

VSP Talk saves the client password in encrypted format in the configuration file. You cannot display the password in clear text.

Note:

VSP Talk cannot connect to some privately-configured IM servers at the TLS level without an officially signed X.509 certificate. The X.509 certificate must be signed by a recognized authority; for example: VeriSign, Microsoft, or A.O.L.

The system logs all communication with IM contacts for security audit purposes. To display VSP Talk log entries, enter the ACLI command **`show log file module VSP_TALK`** . All VSP Talk log entries are recorded with event code 0x002bc600.

VSP Talk only allows you to monitor the system health and status of the switch. To preserve system security, you cannot change any configurations using VSP Talk.

VSP Talk IMCLI example

Following is an example of a VSP Talk Instant Messaging Command Line Interface (IMCL)I session between the IM client of an administrator and the IM client of VSP 9000.

Administrator is the user of VSP Talk.

VSP3rdFloorParkWest is VSP 9000 response in VSP Talk.

Note:

You can enter either the full-length command or the abbreviation in IMCLI. Both are depicted in the following example for demonstration only.

Examples of abbreviations

Full-length command	Abbreviation
show khi performance cpu 1	s k p c 1
enable event-notification	e e
disable event-notification	d e

VSP Talk IMCLI session

```
administrator:show sys-info

VSP3rdFloorParkWest:VSP-9012 (3.2.0.0) (DEV) 0 day(s), 02:35:15

administrator:s s

VSP3rdFloorParkWest: (3.2.0.0) (DEV) 0 day(s), 02:35:15

administrator:show khi performance cpu 1

VSP3rdFloorParkWest: Slot:1

Current utilization: 2

5-minute average utilization: 1

5-minute high water mark: 98 (07/05/11 20:56:14)

administrator:s k p c 1

VSP3rdFloorParkWest: Slot:1

Current utilization: 2

5-minute average utilization: 1

5-minute high water mark: 98 (07/05/11 20:56:14)
```

```
administrator: enable event-notification
VSP3rdFloorParkWest: event-notification enabled
administrator: e e
VSP3rdFloorParkWest: event-notification enabled
administrator: disable event-notification
VSP3rdFloorParkWest: event-notification disabled
administrator: d e
VSP3rdFloorParkWest: event-notification disabled
```

Chapter 29: VSP Talk Configuration Using ACLI

Configure VSP Talk to monitor the status and health of Virtual Services Platform 9000 using an instant messaging client.

Configuring VSP Talk

Configure VSP Talk to monitor the status and health of Virtual Services Platform 9000 through an instant messaging (IM) client.

Once configured, VSP Talk allows you to monitor Virtual Services Platform 9000 remotely through a smart phone, computer or other device.

VSP Talk supports connectivity to these IM servers:

- Google Talk
- Avaya IM

VSP Talk supports IPv4 addresses.

Before you begin

- You must configure IP Domain Name Service before you configure VSP Talk.
- You must log on to Application Configuration mode (at the prompt, enter `enable`, at the next prompt enter `config t`, at the Global Configuration prompt enter `application`).
- You must have an account for Virtual Services Platform 9000 through Avaya IM or Google Talk Instant Messaging (IM).
- You must also have an account set up through Avaya IM or Google Talk for each individual who is to become a contact for Virtual Services Platform 9000.
- Avaya recommends you disable VSP Talk before you make a configuration change.

Important:

To disable VSP Talk, enter the command `no vsptalk {gtalk|avaya} enable`.

After you make the configuration changes, to re-enable VSP Talk enter the command `vsptalk {gtalk|avaya} enable`.

If you use the command `no vsptalk`, without the `enable` operator, your IM Group configuration is lost and the system resets all VSP Talk configuration to default.

Procedure

1. Log on to Application Configuration mode (you must already be in Global Configuration mode):
   ```
   application
   ```
2. Create VSP Talk application:
   ```
   vsptalk
   ```
3. Assign a VSP Talk endpoint address:
   ```
   vsptalk endpoint-address {A.B.C.D}
   ```
   The VSP Talk endpoint address must be in the same IP subnet as an existing VSP IP interface, either in-band or out-of-band.

   Do not use an existing VSP IP address, either in-band or out-of-band, as the VSP Talk endpoint address.
4. Enable event notification to receive instant messages on status updates or to have notification on alarm conditions sent to your smart phone, computer or other device:
   ```
   vsptalk event-notification enable
   ```
5. Enable one of the instant messaging client types:
   ```
   vsptalk <avaya|gtalk>
   ```
6. Define the VSP Talk instant messaging client username and password:
   ```
   vsptalk <avaya|gtalk> client username WORD<0-64> password
   WORD<0-200>
   ```

   Note:

   You must use the name@domainname format for the XMPP account user name. That is, the client username must be a fully qualified account name. For example johnsmith@gmaiil.com or bobbrown@avaya.com.
7. Add your administrator fully qualified XMPP IM account name to become a contact to receive and send messages through IM:
   ```
   vsptalk <avaya|gtalk> client add-buddy WORD<0-1024>
   ```

   Note:

   The format for the client add-buddy name is username@domainname; for example: johnsmith@gmail.com (user name plus @ plus account domain name).
8. Configure a server proxy to access the Internet from the network, if necessary:
   ```
   vsptalk <avaya|gtalk> server proxy WORD<0-255>
   ```

Tip:

You may not require a server proxy if you have direct access to the Internet from your network or if you can reach an IM server over Network Address Translation (NAT) services.

9. Enable VSP Talk:

```
vsptalk <avaya|gtalk> enable
```

Example

```
VSP-9012:1>enable

VSP-9012:1(config)#configure terminal

VSP-9012:1(config-app)#application

VSP-9012:1(config-app)#vsptalk

VSP-9012:1(config-app)#vsptalk endpoint-address 192.0.2.154

VSP-9012:1(config-app)#vsptalk event-notification enable

VSP-9012:1(config-app)#vsptalk gtalk

VSP-9012:1(config-app)#vsptalk gtalk client username
vsp9000@gmail.com password ********

VSP-9012:1(config-app)#vsptalk gtalk client add-buddy
administrator1@gmail.com,administrator2@gmail.com
```

Define the proxy server:

```
VSP-9012:1(config-app)#vsptalk gtalk server proxy http://
proxy.yourcompany.com

VSP-9012:1(config-app)#vsptalk gtalk enable
```

Variable descriptions

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

Variable	Value
endpoint-address *{A.B.C.D}* [vrf <*WORD<0–16>]*	Assigns an address for the VSP Talk application to use for communication. Virtual Services Platform 9000 supports IPv4 addresses for the VSP Talk feature. To insulate mission critical applications, assign an address within your network that is separate from mission critical applications and other features.

Variable	Value
	The parameter vrf <*WORD 0–16*> specifies the name of the virtual router for which the endpoint address belongs. This is an optional parameter.
event-notification enable	Enables event notification to receive instant messages on status updates or to allow Virtual Services Platform 9000 to notify you about alarm conditions. The default is enabled.
<*avaya*|*gtalk*>	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: • avaya — Avaya XMPP IM • gtalk — Google Talk **Note:** VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
<*avaya*|*gtalk*>client add-buddy *WORD<0–200>*	Adds your contact XMPP IM account name to become a contact to receive and send messages through instant messaging. *WORD<0–200>* specifies your XMPP IM account name for the IM client. For instance, if you use Google Talk as the VSP Talk IM client your address is a gmail address: administrator1@gmail.com. The maximum number of contacts is 12.
<*avaya*|*gtalk*>client username *WORD<0–64>* password *WORD<0–200>*	Defines the VSP Talk instant messaging client username and password. *WORD<0–64>* specifies the username and *WORD<0–200>* specifies the password. The username for Virtual Services Platform 9000 is the XMPP IM account name used for Virtual Services Platform 9000 in the IM client. **Tip:** XMPP IM account name format is: user name @ account domain name; for example, johnsmith@gmail.com
<*avaya*|*gtalk*> enable	Enables VSP Talk to monitor the health and status of Virtual Services Platform 9000.

Variable	Value
<*avaya*|*gtalk*> server proxy	Configures a server proxy to access the Internet from the network. **Note:** The system supports only HTTP proxy for the proxy operator.

Configuring VSP Talk with IM server information

Optionally, configure Virtual Services Platform 9000 to use the Avaya IM server using the following commands.

You do not need to use the commands below to configure the Google Talk server. The DNS query to the Google Talk server returns all of the information necessary to make the connection.

Note:

The externally-controlled IM servers, such as Google, apply rate limiting to instant messaging messages. Rate limiting prevents you from sending too many messages in a short period of time and can disable your ability to send messages for a short period of time after you reach the server's predetermined limit.

Before you begin

- Log on to Global Configuration mode.
- Log on to Application Configuration mode.
- You must configure VSP Talk on Virtual Services Platform 9000.

Procedure

1. Specify the instant messaging server address:
   `vsptalk <avaya> server address WORD<0-255>`
2. Specify the TCP port for instant messaging:
   `vsptalk <gtalk> server port <1-49151>`

   Note:

   It is not recommended that you change the server port for gtalk and Avaya SCS.
3. Enable the old-style Secure Sockets Layer (SSL) interface:

   The old-style Secure Socket Layer (SSL) interface is a protocol used to encrypt and transmit private documents over the Internet.

Note:

As of Release 3.2 the system supports only HTTP proxy for the proxy operator. You cannot use HTTPS with the proxy operator.

It is not recommended that you change this parameter for gtalk.

```
vsptalk <avaya|gtalk> server ssltype old
```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# application

VSP-9012:1(config-app)# vsptalk avaya server address 198.51.100.30
```

Variable definitions

Use the data in the following table to use the `vsptalk <avaya|gtalk> server` command.

Variable	Value
address *WORD<0–255>*	Specifies the instant messaging server address.
encryption *<as-requested|required>*	Specifies the encryption option. The default is required. It is not recommended that you change this parameter for gtalk.
port *<1–49151>*	Specifies the TCP port for instant messaging. It is not recommended that you change this parameter for gtalk. The default is 5222.
proxy *WORD<0–255>*	Configures a server proxy to connect to the IM server that you configured.
ssltype old	Enables the old-style Secure Sockets Layer interface. SSL is a protocol used to encrypt and transmit private documents over the Internet. It is not recommended that you change this parameter for gtalk. The default is disabled.

Variable	Value
	Note: As of Release 3.2 the system supports only HTTP proxy for the proxy operator. You cannot use HTTPS with the proxy operator.

Displaying VSP Talk Information

You can display information about VSP Talk to help you determine the current configuration.

Some of the information that you can display about VSP talk includes

- VSP Talk global information: global status, endpoint address, endpoint VRF name, notification status
- VSP Talk client information: messenger client type, user name, password, client status, VSP 9000 client group members, which members receive notification information

  Note:

  Passwords display as ********.
- VSP Talk server information: which IM server is in use, server address, TCP port, server status, security interface, encryption type , proxy status

Before you begin

You must configure and enable VSP Talk.

Procedure

1. Display global VSP Talk information:
   ```
   show application vsptalk
   ```
2. Display VSP Talk client information:
   ```
   show application vsptalk client [<gtalk|avaya>]
   ```
3. Display VSP Talk server information:
   ```
   show application vsptalk server [<gtalk|avaya>]
   ```

Example

```
VSP-9012:2#show application vsptalk
================================================================================
                              VspTalk Global Info
================================================================================
          GlobalEnable  : enable
```

```
      EndpointAddress   : 192.0.2.154
      EndpointVrfName   :
   NotificationEnable   : enable
------------------------------------------------------------------------------
VSP-9012:2#show application vsptalk server gtalk
==============================================================================
                              VspTalk Server Info
==============================================================================
          Type   : gtalk
Server Address   :
          Port   : 5222
        Enable   : enable
       Old SSL   : disable
    Encryption   : required

         Proxy   : http://proxy.yourcompany.com

------------------------------------------------------------------------------
```

Variable descriptions

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

Variable	Value
vsptalk	Displays global VSP Talk information.
application client	Show VSP Talk client information.
application client <*gtalk*|*avaya*>	Show client information for IM Group: • gtalk — Google Talk • avaya — Avaya IM
application server	Show VSP Talk server information.
application server <*gtalk*|*avaya*>	Show server information for IM Group: • gtalk — Google Talk • avaya — Avaya IM

Chapter 30: VSP Talk configuration using EDM

Configure VSP Talk to monitor Avaya Virtual Services Platform 9000 using an instant messaging client. Use this application to configure VSP Talk globally as well as your instant messaging client.

Configuring VSP Talk globally

You can configure VSP Talk to remotely monitor the status and health of your switch on your smart phone, computer, or other device through an instant messaging client .

VSP Talk supports connectivity to IM Servers including:

- Google Talk
- Avaya IM

VSP Talk supports IPv4 addresses.

Before you begin

- You must configure IP Domain Name Service before you enable and configure VSP Talk.
- You must have:
  - an IM client account for your switch through one of the supported IM Servers
  - IM client accounts for the individuals who need to monitor the device remotely using IM

About this task

To enable the VSP Talk application on Virtual Services Platform 9000, assign an IP address, and enable notification for monitoring, use this procedure.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Applications**.
2. Click **VSP Talk**.
3. Click the **Globals** tab.
4. Select the **GlobalEnable** check box.

5. In the **EndpointAddress** box, type an IP address that is separate from mission critical applications.

   Assign an endpoint address to VSP Talk that is in the same IP subnet as an existing VSP IP interface, either in-band or out-of-band. Do not use an existing VSP IP address, either in-band or out-of-band, as the VSP Talk endpoint address.

6. Select the **NotificationEnable** check box.

   Note:

   In IMCLI, you must also use the command **`enable event-notification`** for event notification to function properly.

7. Configure other parameters as desired.

Next steps

Important:

Avaya recommends that you disable VSP Talk before you make a configuration change.

To disable VSP Talk using EDM, on the **Talk Client** tab double-click a table cell beneath Enable. Select **false**. Then you can change other parameters and, when you have completed your changes, you can re-enable VSP Talk on the **Talk Client** tab when you double click the same table cell beneath Enable and select **true**.

CAUTION: If you uncheck the **GlobalEnable** check box on the **Globals** tab in EDM, your IM Group configuration is lost.

If you have never created a Talk Client entry, you do not need to disable VSP Talk because enable/disable affects the configuration only after you create a Talk Client entry (either Google Talk or Avaya, or both).

Globals field descriptions

Use the data in the following table to help you use the **Globals** tab.

Name	Description
GlobalEnable	Creates the VSP Talk application on Virtual Services Platform 9000. Once configured VSP Talk allows you to monitor Virtual Services Platform 9000 remotely through Instant Messaging. **Important:** Once you have enabled VSP Talk on the **Globals** tab, if you uncheck the **GlobalEnable** check box your VSP Talk

Name	Description
	configuration is lost and VSP Talk returns to the default settings. However, you can use the EDM **Talk Client** tab to disable VSP Talk. Then you can make your VSP Talk configuration changes and you can re-enable VSP Talk on the **Talk Client** tab. The default is disabled.
EndpointAddress	Specifies the IP address to use for the VSP Talk feature. Virtual Services Platform 9000 supports IPv4 addresses for the VSP Talk feature. **Important:** Do not use the management IP address. You must select an IP address that is part of your network but that is not already tied to mission critical applications on the switch.
EndpointVrfName	Specifies the name of the virtual router to which the endpoint address belongs. This is an optional parameter.
NotificationEnable	Enable event notification to receive instant messages on status updates or to allow Virtual Services Platform 9000 to notify you about alarm conditions. If you enable event notification, after an event occurs on the switch, the event notification appears within the IMCLI window. The default is disabled. **Note:** In IMCLI , you must also use the command **`enable event-notification`** for this option to function properly.

Configuring a VSP Talk client

You can configure VSP Talk to:

- select the instant messaging (IM) client you want to use
- configure the user name and password for the client
- add IM contacts to the client

You can use VSP Talk to remotely monitor the status and health of your switch on your smart phone, computer, or other device through an instant messaging (IM) client.

VSP Talk supports these IM clients:

- Google Talk
- Avaya IM

VSP Talk supports IPv4 addresses.

Before you begin

- You must have an IM client account for Virtual Services Platform 9000 through one of the supported IM clients.
- You must also have IM client accounts for the individuals who need to monitor the device remotely using IM.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Applications**.
2. Click **VSP Talk**.
3. Click the **Talk Client** tab.
4. Click **Insert**.
5. In the **Type** section, choose an instant messaging client.
6. In the **ServerProxy** field, type the IP address or URL of the proxy server that you use to access the Internet.

   Only HTTP proxy is supported. For example: http://co.proxy.avaya.com:8000 or http://192.0.2.1.:8080
7. In the **ClientUsername** field, specify the username for the IM client account that the VSP 9000 device uses to communicate with other IM clients.

   ClientUsername must be a fully qualified XMPP account name. For example: vsp9000@gmail.com or vsp001@usae.avaya.com.

8. In the **ClientPassword** field, specify the password for the IM client account that the VSP 9000 device uses to communicate with other IM clients.
9. In the **ClientMembers** field, type the account names or email addresses for the individuals who need to monitor the device remotely using IM.

   ClientMembers must be a fully qualified XMPP account name, separated by "," without spaces.
10. Select the **Enable** check box.

    If you uncheck the **Enable** check box, it is the equivalent of disabling VSP Talk when you use the ACLI command **`no vsptalk <gtalk|avaya> enable`**.
11. Click **Insert**.

    You can configure VSP Talk with only one client type at a time. You cannot use more than one client type simultaneously. Even though you can insert any available type, you can enable only one.

Talk Client field descriptions

Use the data in the following table to use the **Talk Client** tab.

Name	Description
Type	Select one of the IM clients that is supported on your mobile device or computer, for example: • gtalk • avaya **Note:** You can use only one client type to configure VSP Talk. You cannot use all available client types simultaneously.
ServerAddress	Specifies the IP address for the messaging server.
ServerPort	Specifies the TCP port for messaging. The range is 1 to 49151.
ServerOldSslTypeEnable	Enables the old-style Secure Sockets Layer interface. SSL is a protocol used to encrypt and transmit private documents over the Internet. The default is disabled.

Name	Description
ServerEncryption	Specifies if encryption is required for the messaging interface. The default is required.
ServerProxy	Configure a server proxy to connect to the Internet. **Note:** As of Release 3.2 the system supports only HTTP proxy for the proxy operator. You cannot use HTTPS with the proxy operator.
ClientUsername	Define VSP Talk instant messaging client username on VSP 9000. The username for VSP 9000 is the IM client account for VSP 9000.
ClientPassword	Specifies the password for the IM account that VSP 9000 uses to communicate with other IM clients.
ClientMembers	Specifies the members (contacts) who want to monitor the device remotely through IM. The value can be an IM account name or fully qualified XMPP IM account name. The account name value can be an IM account name. You can configure up to 12 members, with the names separated by commas (,).
Enable	Enables or disables communication for the IM client. The default is disabled.

Chapter 31: ACLI show command reference

This reference information provides show commands to view the operational status of the Avaya Virtual Services Platform 9000.

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.

```
VSP-9012:1#show cli password
        access-level
        aging     90

        min-passwd-len 10
        password-history 3

        ACCESS    LOGIN            STATE
        rwa       rwa              NA
        rw        rw               ena
        l3        l3               ena
        l2        l2               ena
        l1        l1               ena
        ro        ro               ena
        Default Lockout Time       60
        Lockout-Time:
                     IP                  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-9012:1#show basic config
                       setdate : N/A
           mac-flap-time-limit : 500
            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 <cli|sys|web|rmon|vlan|port|qos|mlt|stg|ip|diag|radius|ntp|lacp|naap|cluster|boot|filter|ipv6|slpp|nsna|vsptalk|isis|spbm|cfm>]

The following table explains parameters for this command.

Table 73: Command parameters

Parameter	Description
module <cli|sys|web|rmon|vlan|port|qos|traffic-filter|mlt|stg|ip|ipx|diag|radius|ntp|svlan|lacp|naap|cluster|boot|filter|ipv6|slpp|nsna|vsptalk|isis|spbm|cfm>	Specifies the command group for which you request configuration settings.
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-9012:1#show running-config
Preparing to Display Configuration...
#
# Tue Aug 09 16:51:22 2011 UTC
# box type             : VSP-9012
# software version     : 3.1.0.0 (GA)
# cli mode             : ACLI
#


#ASIC Info :
#Slot #1:
#       Module: 9080CP
#       OXATE CPLD: 10012015
#       OXIDE FPGA: 10040918
#       CATSKILL FPGA: 10052013
#       QE version: QE2000_A0

#Slot #2:
#       Module: 9080CP
#       OXATE CPLD: 10032310
#       OXIDE FPGA: 10040918
#       CATSKILL FPGA: 10052013
#       QE version: QE2000_A0


--More-- (q = quit)
```

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, OSPF (area, interface, neighbors), 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-9012:1#show cli info

cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 65535 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-9012
```

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-9012:#show ftp-access
     max ipv4 sessions : 4
     max ipv6 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 fo this command is as follows.

show sys-info [asic] [card] [fan] [power] [temperature]

The following table explains parameters for this command.

Table 74: Command parameters

Parameter	Description
asic	Specifies information about the application-specific integrated circuit (ASIC) installed on each module.
card	Specifies information about all the installed modules, including cooling modules, and about firmware for the CF devices. The output for the **show sys-info card** command can incorrectly identify the module description for the 9012RC cooling module as 9012SC. This description was programmed in the SEEPROM during manufacturing of early 9012RC cooling modules. These modules will continue to report this information. Newly manufactured modules correctly display 9012RC as the module description.
fan	Specifies information about installed cooling modules.
power	Specifies information about installed power supplies.
temperature	Specifies information about the temperature.

The following example shows partial output from the **show sys-info** command.

```
VSP-9012:1#show sys-info

General Info :

        SysDescr     : VSP-9012 (3.2.0.0) (DEV)
        SysName      : CB-SWB
        SysUpTime    : 0 day(s), 00:29:23
        SysContact   : http://support.avaya.com/
```

```
        SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis            : 9012
        Serial#            :
        H/W Revision       :
        H/W Config         : 01
        NumSlots           : 12
        NumPorts           : 328
        BaseMacAddr        : 00:24:7f:a1:70:00
        MacAddrCapacity    : 4096
        MgmtMacAddr        : 00:24:7f:a1:73:fd
        System MTU         : 1950

Card Info :

        Slot#  CardType           Serial#            Part#  Oper    Admin   Po
r
                                                           Status  Status  St
e
            1    9080CP            PP9268     EC1404007-E6      up      up
n
            4    9048GT        SSCHJY04HX     EC1404003-E6      up      up
n
            9    9024XL          SC037804     EC1404001-E6    down      up
n

SF Info :

        Slot#  CardType           Serial#            Part#  Oper    Admin   Po
r
                                                           Status  Status  St
e
          SF4    9090SF          SC039592     EC1404006-E6      up      up
n

Temperature Info :

              Slot    Highest     Lowest      Alarm   Shutdown
                         Temp       Temp  Threshold  Threshold
                 1         28         24         60         70
                 4         31         26         60         70
              SF 4         29         29         60         70



--More-- (q = quit)
```

Memory size for CPU

Use the **show boot config** command to display the CPU DRAM memory size, in hexadecimal format.

The syntax for this command is as follows: **show boot config general**

The following example shows sample command output.

```
VSP-9012:1#show boot config general
CPU Slot 1:     9080CP
Version:        3.1.0.0
Memory Size:    0x7CCA9000
```

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-9012:1#show ntp statistics
  NTP Server : 192.0.2.22
---------------------------------
                        Stratum : 5
                        Version : 2
           Sync Status : synchronized
          Reachability : reachable
            Root Delay : 0.19053647
             Precision : 0.00003051
       Access Attempts : 1
          Server Synch : 1
           Server Fail : 0
```

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-9012:1#show sys power

================================================================================
                           Chassis Power Information
================================================================================

Chassis Power Status: redundant

        Total     Required  Max
Chassis Chassis   Redundant Allocated Available
Type    Power     Power     Power     Power
--------------------------------------------------------------------------------
9012    3600      1200      1080      2520
--------------------------------------------------------------------------------
```

Power management information

Use the **show sys power global** command to view a summary of the power redundancy settings.

The syntax for this command is as follows.

show sys power global

The following example shows partial sample command output.

```
VSP-9012:1#show sys power global
              Enable     : true
              slot 1     : critical
              slot 2     : critical
              slot 3     : high
              slot 4     : high
              slot 5     : high
              slot 6     : high
              slot 7     : high
              slot 8     : high
              slot 9     : high
              slot 10    : high
              slot 11    : high
              slot 12    : high
              slot SF1   : critical
              slot SF2   : high
```

```
              slot SF3   : high
              slot SF4   : critical
              slot SF5   : high
              slot SF6   : high
              slot AUX1  : high
              slot AUX2  : high
              slot IOFAN1 : critical
              slot IOFAN2 : critical

--More-- (q = quit)
```

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-9012:1#show sys power power-supply

================================================================================
                            Power Supply Information
================================================================================
Power  Type    Input   Serial         Part            Oper   Max
Supply         Voltage Num            Num             Status Power
--------------------------------------------------------------------------------
PS#1   AC      110     08LD03500078                   up     1200
PS#2   AC      110     08LD11500145                   up     1200
PS#3   AC      110     08DJ47000050                   up     1200
--------------------------------------------------------------------------------
```

Slot power details

Use the **show sys power slot** command to view detailed power information for each slot.

The syntax for this command is as follows.

show sys power slot

The following example shows sample command output.

```
VSP-9012:1#show sys power slot

================================================================================
                             Slot Power Consumption
================================================================================
                                                          Max
Slot     Present CardType            Priority    Power  Allocated
```

```
No.                                                 Status Power
-------------------------------------------------------------------------------
1         YES     9080CP              critical    ON     80
2         YES     9080CP              critical    ON     80
3         YES     9048GT              high        ON     350
SF 1      YES                         critical    ON     70
SF 4      YES     9090SF              critical    ON     70
IO-FAN 1  YES     9012FC              critical    ON     150
IO-FAN 2  NO                          critical    OFF    150
SF-FAN 1  YES     9012RC              critical    OFF    65
SF-FAN 2  YES     9012RC              critical    ON     65
-------------------------------------------------------------------------------

===============================================================================
                            Chassis Power Information
===============================================================================

Chassis Power Status: redundant


--More-- (q = quit)
```

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 <action|dns|force-msg|mgid-usage|msg-control|mtu|power|setting|software|stats|topology-ip>

The following table explains parameters for this command.

Table 75: Command parameters

Parameter	Description
action	Shows the configuration for the system action parameter.
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).

Parameter	Description
mtu	Shows system maximum transmission unit (MTU) information.
power	Shows power information for the chassis. Command options are • **global**—power management settings • **power-supply**—power information for each power supply • **slot**—power information for each slot
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 *Avaya Virtual Services Platform 9000 Performance Management*, NN46250-701.
topology-ip	Shows the circuitless IP set.

The following example shows output from the **show sys action** command.

```
VSP_9012:1#show sys action
               cpuswitchover : (N/A)
                resetconsole : (N/A)
               resetcounters : (N/A)
                  resetmodem : (N/A)
```

The following example shows output from the **show sys dns** command.

```
VSP-9012:1#show sys dns
DNS Default Domain Name : VSP9000SJ
Primary DNS Server details:
===========================
         IP address : 111:0:0:0:0:0:0:1
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
```

The following example shows output from the **show sys mgid-usage** command.

```
VSP-9012:1>show sys mgid-usage
        Number of MGIDs used for VLANs : (65)
        Number of MGIDs used for multicast : (0)
        Number of MGIDs used for SPBM : (1)
        Number of MGIDs remaining for VLANs : (4031)
        Number of MGIDs remaining for multicast : (7900)
        Number of MGIDs remaining for SPBM : (99)
```

The following example shows output from the **show sys msg-control** command.

```
VSP-9012:1#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-9012:1>show sys setting
               mgmt-virtual-ip : 192.0.2.31/255.255.255.0
             mgmt-virtual-ipv6 : 0:0:0:0:0:0:0:0/0
                  udp-checksum : enable
                 udpsrc-by-vip : disable
           mroute-stream-limit : disable
                       contact : http://support.avaya.com/
                      location : 211 Mt. Airy Road,Basking Ridge,NJ 07920
                          name : CB-SWA
                      portlock : off
        sendAuthenticationTrap : false
                   autotopology : on
           ForceTopologyIpFlag : false
            clipId-topology-ip : 0
                           mtu : 1950
```

The following example shows output from the **show sys software** command.

```
VSP-9012:1>show sys software

System Software Info :

Default Runtime Config File : /intflash/config.cfg
Config File :
Last Runtime Config Save : Mon Mar 26 12:36:43 2012
Last Runtime Config Save to Slave : Mon Mar 26 12:36:43 2012

Boot Config Table
Version : Build 3.3.0.0_B022 (PRIVATE) on Thu Mar 8 18:00:59 EST 2012
SlaveCpImageSyncState : N/A
PrimaryConfigSource : /intflash/config.cfg
SecondaryConfigSource : /intflash/config.cfg
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : true
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : true
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), Protocol Independent Multicast (PIM), 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-9012:1#show tech

Sys Info:
---------------


General Info :

        SysDescr     : VSP-9012 (3.1.0.0) (GA)
        SysName      : CB-SWA
        SysUpTime    : 0 day(s), 07:45:04
        SysContact   : http://support.avaya.com/
        SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis            : 9012
        Serial#            : SAN1223008S
        H/W Revision       :
        H/W Config         :
        NumSlots           : 12
        NumPorts           : 50
        BaseMacAddr        : 00:24:7f:9f:60:00
        MacAddrCapacity    : 4096

--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-9012:#show telnet-access
     max ipv4 sessions : 8
     max ipv6 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-9012:1#show users
SESSION   USER                ACCESS    IP ADDRESS
Telnet0   rwa                 rwa       192.0.2.24 (current)
Console                       none      ----------
```

Chapter 32: 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 9000.

Port numbering

A port number includes the slot location of the module in the chassis, as well as the port position in the input/output (I/O) module. In Virtual Services Platform 9000, front module slot numbers increase from top to bottom. Power supplies are numbered from left to right, beginning with 1 for the top, far left power supply. The following figure shows slot numbering for the front of a 9012 chassis.

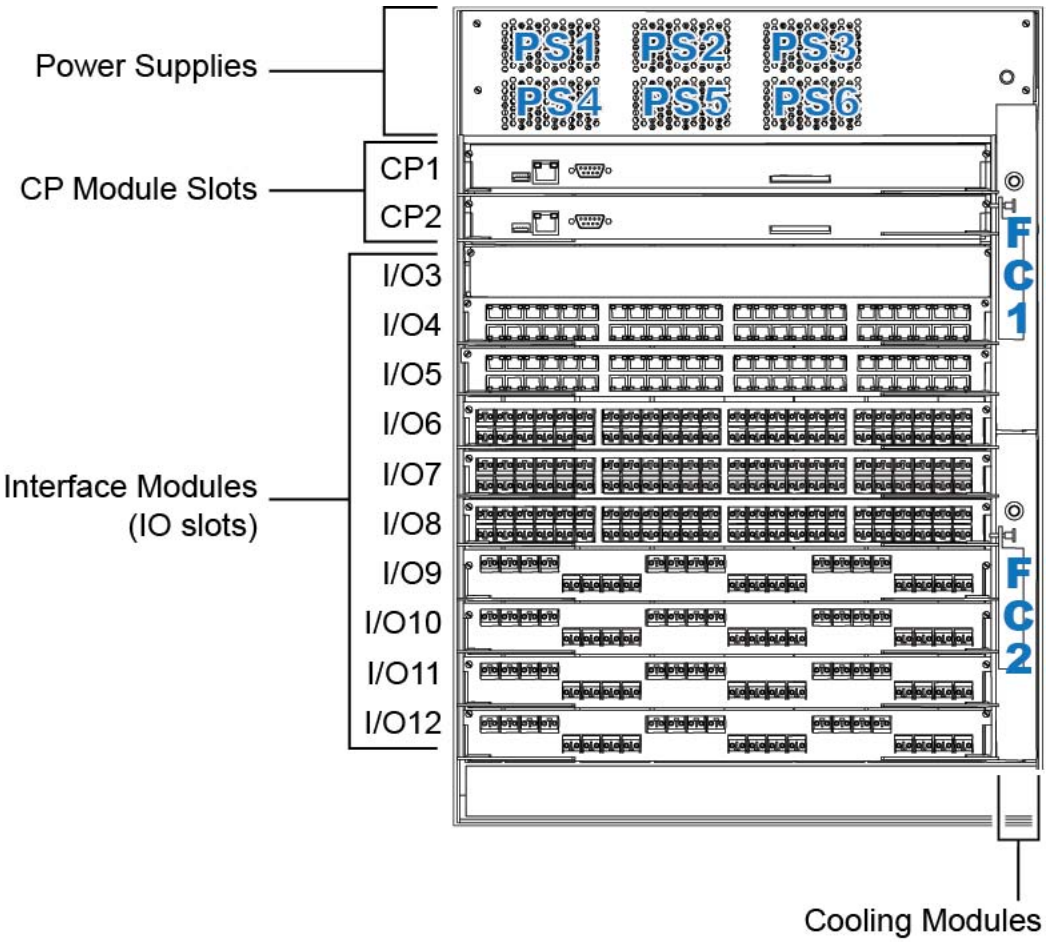

Figure 9: 9012 front chassis slots

The following figure shows slot numbering for the back of a 9012 chassis.

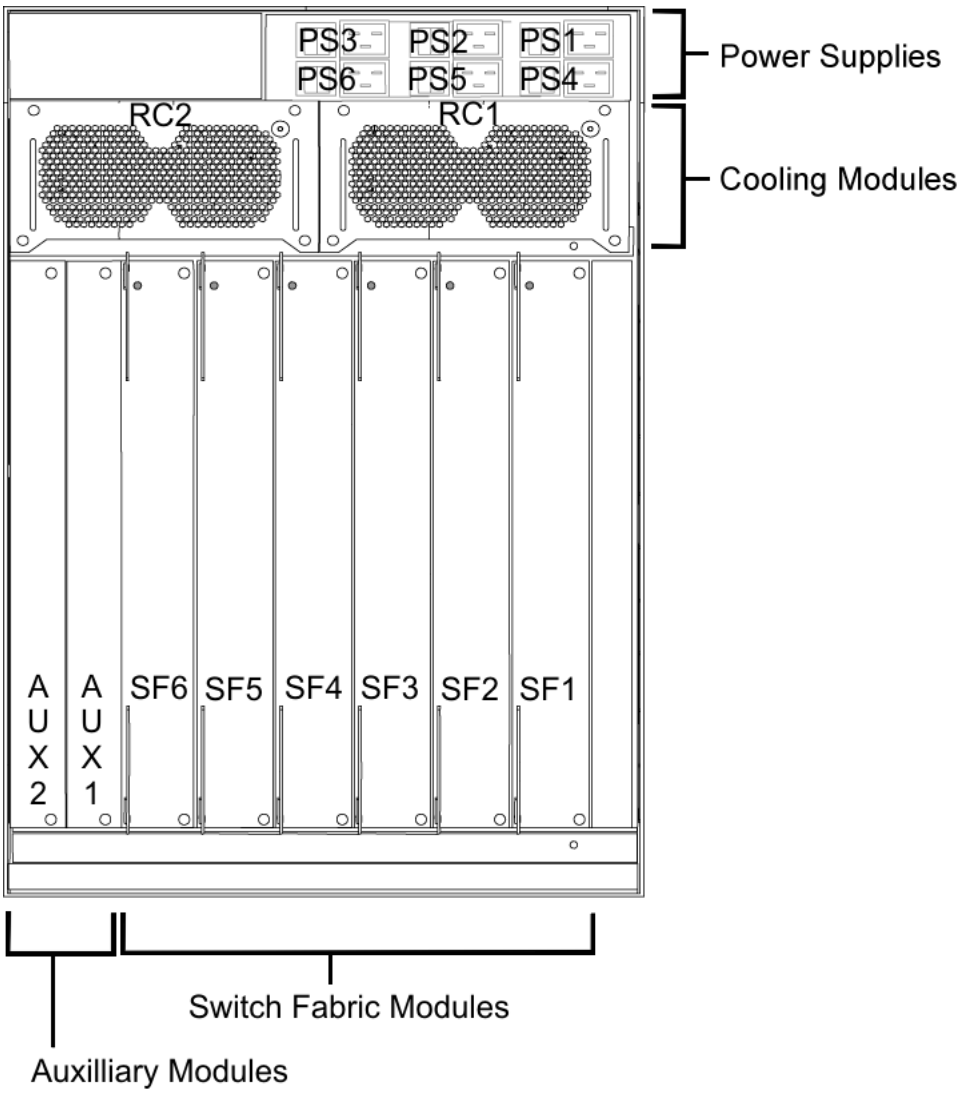

Figure 10: 9012 back chassis slots

Ports are numbered from left to right beginning with 1 for the far left port. On high-density modules with two rows of ports, ports in the top row use sequential odd numbers, and ports in the bottom row use sequential even numbers, see Figure 11: Port numbers on high-density modules on page 279.

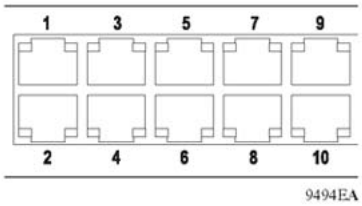

Figure 11: Port numbers on high-density modules

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:

ifIndex = (64 x slot number) + (port number – 1)

Slot number is a value between 1–10, inclusive.

Port number is a value between 1–48, inclusive.

For example, the interface index of port 10/48 is 687.

VLAN interface index

The interface index of a VLAN is computed using the following formula:

ifIndex = 2048 + 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:

ifIndex = 6143 + 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 has a base of 4096 MAC addresses. The system assigns these MAC addresses as follows:

- 512 addresses for ports (physical MAC addresses)
- 3584 addresses for VLANs (virtual MAC addresses).
- 12 addresses for the CPU

A MAC address uses the format shown in the following figure.

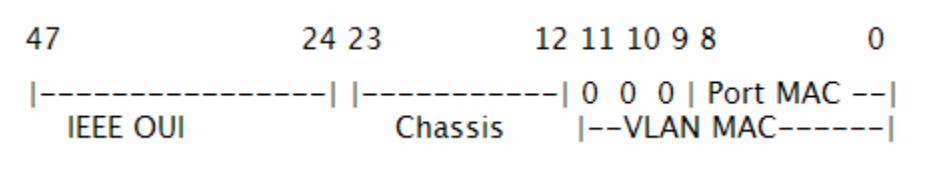

Figure 12: Parts of a MAC address

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, 00-80-2d)
- Bits 23–12: Chassis ID
- Bit 11-9: Type of MAC address in the switch

  If all zeroes (000), it is a port address (physical MAC address); otherwise it is a VLAN address (virtual MAC address)
- Bits 8-0: 512 port MAC addresses
- Bits 11–0: 3584 VLAN MAC addresses

Physical MAC addresses

Physical MAC addresses are addresses assigned to the physical interfaces or ports visible on the device. Frames to or from the physical interface or an isolated routing port use physical MAC addresses.

The ports on the CP module use the following last bytes:

- Management port in slot CP1: 0xf4
- CPU port (an internal port) in slot CP1: 0xf5
- Management port in slot CP2: 0xf6
- CPU port in slot CP2: 0xf7

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 33: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Glossary

Advanced Encryption Standard (AES)	A privacy protocol. U.S. government organizations intend to use AES as the current encryption standard (FIPS-197) to protect sensitive information.
American Standard Code for Information Interchange (ASCII)	A code for representing characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.
application-specific integrated circuit (ASIC)	An application-specific integrated circuit developed to perform more quickly and efficiently than a generic processor.
bit error rate (BER)	The ratio of the number of bit errors to the total number of bits transmitted in a given time interval.
Control Processor Unit High Availability (CPU-HA)	Activates two CP modules simultaneously. The CP modules exchange topology data so, if a failure occurs, either CP module can take precedence in less than 1 second with the most recent topology data.
Circuitless IP (CLIP)	A virtual interface that does not map to any physical interface. This interface is often called a *loopback*.
Custom AutoNegotiation Advertisement (CANA)	An enhancement of the IEEE 802.3 autonegotiation process on the 10/100/1000 copper ports. Custom AutoNegotiation Advertisement offers improved control over the autonegotiation process. The system advertises all port capabilities that include, for tri-speed ports, 10 Mb/s, 100 Mb/s, 1000 Mb/s speeds, and duplex and half-duplex modes of operation. This advertisement results in autonegotiation between the local and remote end that settles on the highest common denominator. Custom AutoNegotiation Advertisement can advertise a user-defined subset of the capabilities that settle on a lower or particular capability.
Data Terminating Equipment (DTE)	A computer or terminal on the network that is the source or destination of signals.
denial-of-service (DoS)	Attacks that prevent a target server or victim device from performing its normal functions through flooding, irregular protocol sizes (for example, ping requests aimed at the victim server), and application buffer overflows.
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)	A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).
Dynamic Random Access Memory (DRAM)	A read-write random-access memory, in which the digital information is represented by charges stored on the capacitors and must be repeatedly replenished in order to retain the information.
File Transfer Protocol (FTP)	A protocol that governs transferring files between nodes, as documented in RFC 959. FTP is not secure. FTP does not encrypt transferred data. Use FTP access only after you determine it is safe in your network.
forwarding database (FDB)	A database that maps a port for every MAC address. If a packet is sent to a specific MAC address, the switch refers to the forwarding database for the corresponding port number and sends the data packet through that port.
Generalized Regular Expression Parser (grep)	A Unix command used to search files for lines that match a given regular expression (RE).
Institute of Electrical and Electronics Engineers (IEEE)	An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.
Interface module	An interface module is a module that provides network connectivity for various media (sometimes called Layer 0) and protocol types. Interface modules are also called Ethernet modules.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Internet Group Management Protocol (IGMP)	A host membership protocol used to arbitrate membership in multicast services.
interswitch trunking (IST)	A feature that uses one or more parallel point-to-point links to connect two aggregation switches. The two aggregation switches use this channel to share information and operate as a single logical switch. Only one interswitch trunk can exist on each Split Multilink Trunking (SMLT) aggregation switch.
Layer 1	The Physical Layer of the Open System Interconnection (OSI) model. Layer 1 interfaces with the MAC sublayer of Layer 2, and performs character encoding, transmission, reception, and character decoding.
Layer 2	The Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.

Layer 3	The Network Layer of the OSI model. Example of a Layer 3 protocol is Internet Protocol (IP).
Link Aggregation Control Protocol (LACP)	A protocol that exists between two endpoints to bundle links into an aggregated link group for bandwidth increase and link redundancy.
Local Area Network (LAN)	A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).
management information base (MIB)	Defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
mask	A bit string that is used along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
maximum transmission unit (MTU)	The largest number of bytes in a packet—the maximum transmission unit of the port.
media	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
Message Digest 5 (MD5)	A one-way hash function that creates a message digest for digital signatures.
multicast group ID (MGID)	The multicast group ID (MGID) is a hardware mechanism the switch uses to send data to several ports simultaneously. Instead of sending the data to a specific port number, the data is directed to an MGID. The switch maintains a table that maps MGIDs to their member ports. Both virtual LAN (VLAN) and IP multicast (IPMC) use MGIDs.
MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
multimode fiber (MMF)	A fiber with a core diameter larger than the wavelength of light transmitted that you can use to propagate many modes of light. Commonly used with LED sources for low speed and short distance lengths. Typical core sizes (measured in microns) are 50/125, 62.5/125 and 100/140.
nanometer (nm)	One billionth of a meter (10^{-9} meter). A unit of measure commonly used to express the wavelengths of light.

Network Time Protocol (NTP)	A protocol that works with TCP that assures accurate local time keeping with reference to radio and atomic clocks located on the Internet. NTP synchronizes distributed clocks within milliseconds over long time periods.
NonVolatile Random Access Memory (NVRAM)	Random Access Memory that retains its contents after electrical power turns off.
out of band (OOB)	Network dedicated for management access to chassis.
Packet Capture Tool (PCAP)	A data packet capture tool that captures ingress and egress (on Ethernet modules only) packets on selected ports. You can analyze captured packets for troubleshooting purposes.
port	A physical interface that transmits and receives data.
Protocol Data Units (PDUs)	A unit of data that is specified in a protocol of a given layer and that consists of protocol-control information of the given layer and possibly user data of that layer.
Protocol Independent Multicast, Source Specific (PIM-SSM)	Uses only shortest-path trees to provide multicast services based on subscription to a particular (source, group) channel.
Protocol Independent Multicast, Sparse Mode (PIM-SM)	Adds a Rendezvous Point router to avoid multicast-data flooding. Use PIM-SM when receivers for multicast data are sparsely distributed throughout the network.
quality of service (QoS)	Use QoS features to reserve resources in a congested network. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are important than the file transfers.
Read Write All (RWA)	An access class that lets users access all menu items and editable fields.
remote login (rlogin)	An application that provides a terminal interface between hosts (usually UNIX) that use the TCP/IP network protocol. Unlike Telnet, rlogin assumes the remote host is, or behaves like, a UNIX host.
remote monitoring (RMON)	A remote monitoring standard for Simple Network Management Protocol (SNMP)-based management information bases (MIB). The Internetwork Engineering Task Force (IETF) proposed the RMON standard to provide guidelines for remote monitoring of individual LAN segments.

Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. The RIP is most often used as a very simple IGP within small networks.
Secure Copy (SCP)	Securely transfers files between the switch and a remote station.
Secure Shell (SSH)	Used for secure remote logons and data transfer over the Internet. SSH uses encryption to provide security.
Simple Loop Prevention Protocol (SLPP)	Simple Hello Protocol that prevents loops in a Layer 2 network (VLAN).
Simple Network Management Protocol (SNMP)	Administratively monitors network performance through agents and management stations.
single mode fiber (SMF)	One of the various light waves transmitted in an optical fiber. Each optical signal generates many modes, but in single-mode fiber only one mode is transmitted. Transmission occurs through a small diameter core (approximately ten micrometers), with a cladding that is 10 times the core diameter. These fibers have a potential bandwidth of 50 to 100 GHz per kilometer.
small form factor pluggable (SFP)	A hot-swappable input and output enhancement component used with Avaya products to allow gigabit Ethernet ports to link with other gigabit Ethernet ports over various media types.
SMLT aggregation switch	One of two IST peer switches that form a split link aggregation group. It connects to multiple wiring closet switches, edge switches, or customer premise equipment (CPE) devices.
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Group (STG)	A collection of ports in one spanning tree instance.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
trunk	A logical group of ports that behaves like a single large port.
universal asynchronous	A device that converts outgoing parallel data to serial transmission and incoming serial data to parallel for reception.

receiver-transmitter (UART)	
user-based security model (USM)	A security model that uses a defined set of user identities for authorized users on a particular Simple Network Management Protocol (SNMP) engine.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
virtual router forwarding (VRF)	Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by providing separate routing functionality, and the network treats each VRF as a separate physical router.
Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.