AVAYA

Administering VSP Operating System Software

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

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

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Contents

Chapter 1: Introduction

Purpose

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

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

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

This document includes both initial and ongoing administrative tasks for the switches.

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Chapter 2: New in this document

The following sections detail what is new in *Administering*.

> **Important:**
>
> The features in this document might not apply to all hardware platforms. For more information about feature support, see *Release Notes*.

Release 6.0.1

Saving configuration before system shutdown

Clarification information is added to the procedure Shutting down the system on page 30. You must follow this procedure to ensure that you do not lose recently saved configuration after reboot.

SSL certificate format

The section Secure Shell fundamentals on page 214 is updated to indicate the required encoding format if you need to use your own SSL certificate.

Release 6.0

Boot configuration flags

Several new features impact the boot configuration flags. For more information, see the following information:

- System flags on page 55
- Configuring boot flags on page 66 for a CLI procedure.
- Configuring boot flags on page 125 for an EDM procedure.
- Displaying the boot config flags status on page 260

EDM support for viewing licenses

You can now use EDM to view information about the license file on the switch. For more information, see Viewing license file information on page 174.

Entity MIB - Physical Table

The Entity MIB - Physical Table assists in the discovery of functional components on the switch. The Entity MIB - Physical Table supports a physical interface table that includes information about the chassis, power supply, fan, I/O cards, console, and management port.

Image upgrade

The information in the Image upgrade on page 15 chapter was relocated from the Release Notes into this document.

Inclusion of VSP 4000

VOSS 6.0 updates this document to include the VSP 4000 Series. This document is now the single *Administering* document for all VOSS platforms.

IEEE 802.3X Pause frame transmit

This release introduces support for flow control mode and the ability for an interface to send pause frames. When congestion occurs on an egress port, the system can send pause frames to the offending devices to stop the packet flow. The system uses flow control if the rate at which one or more ports receives packets is greater than the rate at which the switch transmits packets.

For more information, see the following sections:

- IEEE 802.3X Pause frame transmit on page 92
- Configuring IEEE 802.3X Pause frame transmit on page 102 for a CLI procedure.
- Configuring IEEE 802.3X Pause frame transmit on page 121 for an EDM procedure.

Increased VRF and Layer 3 VSN scaling

You can now use a boot config flag to increase the number of Virtual Routing and Forwarding (VRF) instances on the switch from the previous maximum of 24. This enhancement also impacts the number of Layer 3 Virtual Services Networks (VSN). The maximum number of supported VRFs and Layer 3 VSNs differs depending on the hardware platform.

For more information about maximum scaling numbers, see *Release Notes*.

For more information, see the following sections:

- System flags on page 55
- Configuring boot flags on page 66 for a CLI procedure.
- Configuring boot flags on page 125for an EDM procedure.

Licensing

Licensing information is updated for new features as applicable. For more information, see Licensing on page 164.

Link Layer Discovery Protocol (LLDP)

This release introduces support for Link Layer Discovery Protocol (LLDP) which has been standardized by the IEEE as part of 802.1ab. LLDP enables you to advertise your identity and capabilities and obtain the same information from a physically adjacent Layer 2 peer to detect and correct network and configuration errors.

For more information, see Link Layer Discovery Protocol (802.1AB) fundamentals on page 176.

MACsec enhancements

MACsec updates in this release enable enhanced security where multiple Secure Association (SA) Keys are internally derived from the configured Connectivity Association Key (CAK), to secure communication on the link. These SA Keys are periodically refreshed to ensure that the same key is not used for an extended period of time. From a provisioning perspective, the administrator still configures a single shared CAK on the two ends of the MACsec enabled link. This CAK is now used to internally derive multiple SA Keys. In order to differentiate the transmit and receive SA keys used between two ends of a MACsec enabled link, one additional parameter has been added (`key-parity <even|odd>`). MACsec links should always be provisioned as odd/even pair.

For more information, see Downloading the software on page 226.

nni-mstp boot flag configuration support

The default value for the nni-mstp flag is false. In previous releases, MSTP was enabled for the CIST and all MSTIs other than MSTI-62. In the current release, the default behavior of the MSTP on SPBM NNI ports is that CIST is disabled automatically on the NNI and the NNI ports cannot be members of any VLANs other than B-VLANs. You can override this by setting the nni-mstp flag to true, which disables MSTP on MSTI-62, and allows any VLAN to be configured on NNI ports.

On SPBM NNI links, MSTP is disabled and no VLAN, except SPBM B-VLANs can be added. When nni-mstp flag is set to true, it only disables MSTI 62 and additional VLANs on other MSTIs can be added to NNI links.

For more information, see nni-mstp boot config flag on page 50.

Resources

Information about related resources is moved to the last chapter in this document.

SMTP for email notification

The switch supports the SMTP feature to send email notification of failed components or other critical log-event conditions. The switch can also send periodic health status notifications.

For more information, see Supported RFCs on page 308.

SSH client disable

This release adds the ability to disable the SSH client in the software.

For more information, see Enabling or disabling the SSH client on page 238.

Chapter 3: Image upgrade

This section details what you must know to upgrade the switch.

Upgrades

Install new software upgrades to add functionality to the switch. Major and minor upgrades are released depending on how many features the upgrade adds or modifies.

Upgrade time requirements

Image upgrades take less than 30 minutes to complete. The switch continues to operate during the image download process. A service interruption occurs during the installation and subsequent reset of the device. The system returns to an operational state after a successful installation of the new software and device reset.

Before you upgrade the software image

Before you upgrade the switch, ensure that you read the entire upgrading procedure.

You must keep a copy of the previous configuration file (*config.cfg*), in case you need to return to the previous version. The upgrade process automatically converts, but does not save, the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.

Image naming conventions

The switch software use a standardized dot notation format.

Software images

Software image names use the following number format to identify release and maintenance values:

Product Name.Major Release.Minor Release.Maintenance Release.Maintenance Release Update.tgz

For example, the image file name **VOSS4K.4.2.1.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 4, a minor release version of 2, a maintenance release version of 1 and a maintenance release update version of 0. Similarly, the image file name **VSP4K. 3.0.1.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 3, a minor release version of 0, a maintenance release version of 1 and a maintenance release update version of 0. TGZ is the file extension.

Interfaces

You can apply upgrades to the switch using the Command Line Interface (CLI).

For more information about CLI, see *Using CLI and EDM*.

File storage options

This section details what you must know about the internal boot and system flash memory and Universal Serial Bus (USB) mass-storage device, which you can use to store the files that start and operate the switch.

The switch file system uses long file names.

Internal flash

The switch has two internal flash memory devices: the boot flash memory and the system flash memory. The system flash memory size is 2 gigabytes (GB).

Boot flash memory is split into two banks that each contain a different copy of the boot image files. Only the Image Management feature can make changes to the boot flash.

The system flash memory stores configuration files, runtime images, the system log, and other files. You can access files on the internal flash through the /intflash/ folder.

USB device

The switch can use a USB device for additional storage or configuration files, release images, and other files. The USB device provides a convenient, removable mechanical to copy files between a computer and a switch, or between switches. In cases where network connectivity has not yet been established, or network file transfer is not feasible, you can use a USB device to upgrade the configuration and image files on the switch.

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

File Transfer Protocol

You can use File Transfer Protocol (FTP) to load the software directly to the switch, or to download the software to the internal flash memory or to an installed USB device.

The switch can act as an FTP server or client. If you enable the FTP daemon (ftpd), you can use a standards-based FTP client to connect to the switch by using the CLI log on parameters. Copy the files from the client to either the internal flash memory or USB device.

Important upgrade note for systems using IPv6 static neighbors

Due to an issue in VOSS 4.2.1 and later releases, the port number for an IPv6 static neighbor is saved with the wrong value in the configuration file if the port is part of an MLT or SMLT. You can view the incorrect port number by using the `show running-config` command.

If performing a named boot (e.g. `boot config.cfg`), the configuration loading fails and the switch remains in a default configuration. You can manually source the configuration file (e.g. `source config.cfg`) to retrieve/reapply the configuration (minus the IPv6 neighbor configuration with the invalid port value).

If you boot the switch without a specified configuration (e.g. `reset -y`), the primary configuration fails to load and the backup configuration file is loaded instead.

⚠️ **Caution:**

> You should never configure an IPv6 static neighbor on a port belonging to an MLT or SMLT.

Pre-upgrade instructions for IS-IS metric type

The command used to redistribute routes into IS-IS supports a parameter called metric-type, which can take one of two values: internal or external. In releases that do not support the external metric type, the routes are always advertised into IS-IS as internal, irrespective of whether you configure the metric-type to internal or external. The saved configuration itself correctly shows the value that you selected.

If the configuration file has redistribution commands that set the metric-type to external, after you upgrade to a release that supports the external metric type, the routes will be advertised into IS-IS as external routes. This constitutes a change in how the routes are advertised into IS-IS after the upgrade as compared to before the upgrade. This configuration can cause unintended traffic issues if the other switches in the network are not yet upgraded to a release that recognizes external routes in IS-IS.

To know which release supports the external metric type on your platform, see *Release Notes*.

To avoid unintentionally impacting traffic immediately following an upgrade, it is recommended that the existing IS-IS redistribution configuration of a switch be checked prior to the upgrade to determine if the metric-type is set to external in the redistribution commands. If metric-type external is not used in the redistribution, the switch can be upgraded using the normal upgrade procedures. If the metric-type external is used with any redistribution command, change it to internal, and then save the configuration. After this the switch can be upgraded using the normal upgrade procedures.

Commands to check metric-type in redistribution configuration:

```
Switch:1(config-isis)#show ip isis redistribute [vrf WORD<1-16>]
================================================================================
  ISIS Redistribute List - GlobalRouter
================================================================================
SOURCE MET MTYPE      SUBNET    ENABLE LEVEL  RPOLICY
```

```
--------------------------------------------------------------------------------
RIP    0   internal   allow     TRUE   l1
OSPF   0   external   allow     TRUE   l1
LOC    0   external   allow     TRUE   l1
```

Commands to change metric-type to internal for GRT:

```
router isis
isis redistribute <protocol> metric-type internal
save config
```

The *protocol* above could be one of **direct**, **ospf**, **static**, **rip** or **bgp**.

Commands to change metric-type to internal for VRF:

```
router vrf WORD<1-16>
isis redistribute <protocol> metric-type internal
save config
```

The *protocol* above could be one of **direct**, **ospf**, **static**, **rip** or **bgp**.

Important upgrade consideration regarding MACsec

The switch software does not support nor display the replay-protect option within MACsec. In some early releases, the replay-protect option is still visible and configurable, even though it is not supported. If you configured the replay-protect option in an early release, follow the steps mentioned below to carefully disable replay-protect before you upgrade the switch software to a release where the option is no longer visible.

⚹ **Note:**

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

About this task

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

Procedure

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

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

   a. Disable MACsec replay-protect on the remote end of the MACsec enabled the link.

   b. Disable MACsec replay-protect on the local end of the MACsec enabled link.

   c. Save the configuration on both nodes.

   d. Start the software upgrade.

Upgrading to support the nni-mstp boot flag

If you upgrade to a release that supports the mstp default behavior change that is associated with the boot config flags nni-mstp, and your previous configuration included coexistence of MSTP and SPB-based services on the NNI ports in the configuration file, take note of the following:

During startup, your configuration file continues to load successfully but now it includes a change that set the nni-mstp flag to true (if it was not already set to true). Your system operates the same as before the upgrade.

After startup, save the configuration file. If you do not save your configuration, you continue to see the following message on reboot.

```
 Warning
Detected brouter and/or vlans other than BVLANs on NNI ports. Setting the boot config
flag nni-mstp to true. Saving configuration avoids repetition of this warning on reboot.
```

Saving the configuration

Save the configuration

- When you make a change to the configuration.
- To create a backup configuration file before you upgrade the software on the switch.

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

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support IPv4 and IPv6 addresses.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

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

Example

```
Switch:1> enable
```

Save the configuration to the default location:

```
Switch:1# save config
```

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

```
Switch:1# save config backup /usb/PreUpgradeBackup.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 format: • a.b.c.d:<file> • /intflash/<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 format: • a.b.c.d:<file> • /intflash/<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.

Upgrading the software

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

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

• Use FTP or SFTP to transfer the file.

• Download the file to your computer. Copy the file to a USB device and insert the USB device into the USB port on the switch.

  🛈 **Important:**

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

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

For information about how to remove a software release, see

Before you begin

- To obtain the new software, go to the Avaya support site: www.avaya.com/support. You need a valid user or site ID and password.

- Back up the configuration files.

- Use an FTP or SFTP application or USB device to transfer the file with the new software release to the switch.

- Ensure that you have not configured a VLAN above 4059. If you have, you must port all configuration on this VLAN to another VLAN, before you begin the upgrade.

  ⚠️ **Caution:**

  Only VLAN range 2 to 4059 is supported. All configuration on a higher numbered VLAN from earlier releases will be lost after the upgrade.

- Check the MACsec configuration on the device prior to upgrading. For more information, see Important upgrade consideration regarding MACsec on page 18.

- If you plan to upgrade from either Release 4.2.1.0 or 4.2.1.1 to 5.0 or later and have IS-IS-enabled links with HMAC-MD5 authentication, use the `no isis hello-auth` command to disable IS-IS authentication one link at a time for all systems. Ensure each link is stable before you move on to the next link. After you have disabled all IS-IS authentication, save the configuration, and then perform the upgrade. After the upgrade is complete, you can reenable IS-IS authentication one link at a time, and then save the configuration on each switch.

✴️ **Note:**

Software upgrade configurations are case-sensitive.

About this task

🛈 **Important:**

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

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

> ⭐ **Note:**
>
> Start an FTP session from your computer to the switch using the same username and password used to Telnet or SSH to the switch. Upload or copy the image to the switch.

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

```
end
```

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

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

```
exit
```

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

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

6. Install the image:

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

7. Restart the switch:

```
reset
```

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

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

rwa

```
enable
```

9. Confirm the software is upgraded:

```
show software
```

10. Commit the software:

```
software commit
```

Example

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

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags ftpd
Switch:1(config)#end
Switch:1(config)#copy /usb/VOSS8K.6.0.0.0.tgz /intflash/VOSS8K.6.0.0.0.tgz
Switch:1(config)#exit
Switch:1#software add VOSS8K.6.0.0.0.tgz
Switch:1#software activate VOSS8K.6.0.0.0.GA
Switch:1#reset
Switch:1#show software
================================================================================
                      software releases in /intflash/release/
================================================================================
VOSS8K.5.0.0.0.GA (Primary Release)
VOSS8K.4.2.1.0.GA (Backup Release)


--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes

Switch:1#show software detail

================================================================================
                      software releases in /intflash/release/
================================================================================
VOSS8K.4.2.1.0.GA (Backup Release)
    KERNEL                          2.6.32_int38
    ROOTFS                          2.6.32_int38
    APPFS                           VOSS8K.4.2.1.0int012
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES


VOSS8K.5.0.0.0.GA (Primary Release)
    KERNEL                          2.6.32_int38
    ROOTFS                          2.6.32_int38
    APPFS                           VOSS8K.5.0.0.0.GA
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES




--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes

Switch:1#software commit
```

Verifying the upgrade

Verify your upgrade to ensure proper switch operation.

Procedure

1. Check for alarms or unexpected errors:

   ```
   show logging file tail
   ```

2. Verify all modules and slots are online:

   ```
   show sys-info
   ```

Committing an upgrade

Perform the following procedure to commit an upgrade.

About this task

The commit function for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure that the upgrade is successful. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version. By default, auto-commit is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```
   ```
   configure terminal
   ```

2. **(Optional)** Configure the timer to activate the software:

   ```
   sys software commit-time <10-60>
   ```

   The default is 10 minutes.

3. **(Optional)** Extend or reduce the time to commit the software:

   software reset-commit-time [<1–60>]

4. Commit the upgrade:

   ```
   software commit
   ```

Downgrading the software

Perform this procedure to downgrade the switch from the current trusted version to a previous release.

! Important:

In VOSS 4.2 and later, the encryption modules are included in the image file. Therefore, the `load-encryption` command and the `software add-module` command is present but no longer applicable to the current release. You do not require a CLI command to add or load the encryption module. Use the `software add-module` command only if you downgrade to a release earlier than VOSS 4.2.

! Important:

MACsec connectivity association (CA) configurations fail during downgrade. If you plan to downgrade MACsec to an earlier version, delete the MACsec CA entries, perform the downgrade, and then reconfigure the MACsec CA entries. This applies to both 2AN and 4AN modes.

Before you begin

Ensure that you have a previous version installed.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Extract the release distribution files to the /intflash/release/ directory:

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

3. Extract the module files to the /intflash/release directory:

   ```
   Software add-module [software version] [modules file name]
   ```

   ✱ Note:

   This step applies to downgrades to a software version earlier than VOSS 4.2.

4. Activate a prior version of the software:

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

5. Restart the switch:

   ```
   reset
   ```

   ! Important:

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

6. Commit the software change:

   ```
   software commit
   ```

> **❗ Important:**
>
> If you do not enable the auto-commit functionality, you must commit the software change before the commit timer expires. This is an optional step otherwise.

7. Verify the downgrade:

    - Check for alarms or unexpected errors using the `show logging file tail` command.
    - Verify all modules and slots are online using the `show sys-info` command.

8. **(Optional)** Remove unused software:

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

Variable definitions

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

Variable	Value
activate WORD<1-99>	Specifies the name of the software release image.
add WORD<1-99>	Specifies the path and version of the compressed software release archive file.
remove WORD<1-99>	Specifies the path and version of the compressed software release archive file.

Deleting a software release

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

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

Procedure

1. Enter Privileged EXEC configuration mode:

    ```
    enable
    ```

2. Remove software:

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

Example

The following steps are just an example. The same steps apply to other switches.

```
Switch:1>enable
```

```
Switch:1#software remove VSP4K.4.1.0.0
```

Upgrading the boot loader image

⚠️ **Warning:**

This command is an advanced-level command that upgrades the device uboot image. Only use this command if specifically advised to do so by Technical Support. Improper use of this command can result in permanent damage to the device and render it unusable.

If the need to use this command arises, instructions on usage will be provided by technical support.

Before you begin

- Transfer the image to the `/intflash/` directory on the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the current uboot version:

   ```
   show sys-info uboot
   ```

3. Upgrade the boot loader image:

   ```
   uboot-install WORD<1-99>
   ```

Variable definitions

Use the data in the following table to use the **uboot-install** command.

Variable	Value
WORD<1-99>	Specifies the full path and filename that contains the uboot image.

Chapter 4: Basic administration

The following sections describe common procedures to configure and monitor the switch.

Basic administration procedures using CLI

The following section describes common procedures that you use while you configure and monitor the switch operations using the Command Line Interface (CLI).

> **✳ Note:**
>
> Unless otherwise stated, to perform the procedures in this section, you must log on to the Privileged EXEC mode in the CLI. For more information about how to use CLI, see *Using CLI and EDM*.

Restarting the platform

Before you begin

- > **✳ 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 config file name. If you do not specify a boot source and file, the boot command uses the configuration files on the primary boot device defined by the `boot config choice` command.

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Restart the switch:

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

> ⓘ **Important:**
>
> If you enter the `boot` command with no arguments, you cause the switch to start using the current boot choices defined by the `boot config choice` command.
>
> If you enter a boot command and the configuration file name without the directory, the device uses the configuration file from /intflash/.

Example

```
Switch:1> enable
```

Restart the switch:

```
Switch:1# boot config /intflash/config.cfg

Switch:1# Do you want to continue? (y/n)

Switch:1# Do you want to continue? (y/n) y
```

Variable definitions

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

Variable	Value
config WORD<1–99>	Specifies the software configuration device and file name in one of the following formats: • /intflash/ <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

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Reset the switch:

   ```
   reset [-y]
   ```

Example

```
Switch:1> enable
```

Reset the switch:

```
Switch: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.

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

Shutting down the system

Use the following procedure to shut down the system.

⚠️ **Caution:**

Before you unplug the AC power cord, always perform the following shutdown procedure.

This procedure:

- Flushes any pending data to ensure data integrity.
- Ensures the completion of recent configuration save actions, thus preventing the system from inadvertently booting up with incorrect configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Shut down the system:

   ```
   sys shutdown
   ```

3. Before you unplug the power cord, wait until you see the following message:

   ```
   System Halted, OK to turn off power
   ```

Example

Shut down a running system.

```
Switch:1#sys shutdown
Are you sure you want shutdown the system? Y/N  (y/n) ? y
CP1  [05/08/14 15:47:50.164] 0x00010813 00000000 GlobalRouter HW INFO System shutdown
initiated from CLI
CP1  [05/08/14 15:47:52.000] LifeCycle: INFO: Stopping all processes
```

```
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All processes have stopped
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All applications shutdown, starting power
down sequence
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none killed
Stopping vsp...Error, do this: mount -t proc none /proc
done
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
Deconfiguring network interfaces... done.
Stopping syslogd/klogd: no syslogd found; none killed
Sending all processes the TERM signal...
Sending all processes the KILL signal...
/etc/rc0.d/S25save-rtc.sh: line 5: /etc/timestamp: Read-only file system
Unmounting remote filesystems...
Stopping portmap daemon: portmap.
Deactivating swap...
Unmounting local filesystems...
[24481.722669] Power down.
[24481.751868] System Halted, OK to turn off power
```

Pinging an IP device

About this task

Ping a device to test the connection between the switch and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address does not respond.

Procedure

1. Log on to the switch to enter User EXEC mode.

2. Ping an IP network connection:

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

Example

Ping an IP device from a GRT VLAN IP interface:

Switch:1# ping 192.0.2.16

192.0.2.16 is alive

Variable definitions

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

Variable	Value
count <1–9999>	Specifies the number of times to ping (1–9999).
-d	Configures the ping debug mode. This variable detects local software failures (ping related threads creation or write to sending socket) and receiving issues (ICMP packet too short or wrong ICMP packet type).
datasize {28-9216|28–51200}	Specifies the size of ping data sent in bytes. The datasize for IPv4 addresses is *<28-9216>*. The datasize for IPv6 addresses is *<28-51200>*. The default is 0.
interface <gigabitEthernet	mgmtEthenet	tunnel	vlan>	Configures a specific outgoing interface to use by IP address. Additional ping interface filters: • gigabitEthernet: {slot/port[/sub-port]} gigabit ethernet port • mgmtEthenet: {slot/port[/sub-port]} mgmt ethernet port. • tunnel: tunnel ID as a value from 1–2000 • vlan: Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3999. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
-I <1–60>	Specifies the interval between transmissions in seconds (1–60).
scopeid <1–9999>	Specifies the scope ID. *<1–9999>* specifies the circuit ID for IPv6.
-s	Configures the continuous ping at the interval rate defined by the [-I] parameter.
source WORD *<1–256>*	Specifies an IP address to be used as the source IP address in the packet header.
-t <1–120>	Specifies the no-answer timeout value in seconds (1–120).
vrf WORD<0–16>	Specifies the virtual routing and forwarding (VRF) name from 1–16 characters.
WORD<0–256>	Specifies the host name or IPv4 (a.b.c.d) address (string length 0–256). Specifies the address to ping.

Calculating and verifying the md5 checksum for a file on a switch

Perform this procedure on a VSP switch to verify that the software files downloaded properly to the switch. Avaya provides the md5 checksum for each release on the Avaya Support website.

Before you begin

- Download the md5 checksum to an intermediate workstation or server where you can open and view the contents.
- Download the .tgz image file to the switch.

About this task

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

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Use the **ls** command to view a list of files with the `.tgz` extension:

   ```
   ls *.tgz
   ```

3. Calculate the md5 checksum for the file:

   ```
   md5 <filename.tgz>
   ```

4. Compare the number generated for the file on the switch with the number that appears in the md5 checksum on the workstation or server. Ensure that the md5 checksum of the software suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

The following example provides output for VSP 8200 but the same process can be used on other VSP switches.

View the contents of the md5 checksum on the workstation or server:

```
3242309ad6660ef09be1b945be15676d   VSP8200.4.0.0.0_edoc.tar
d000965876dee2387f1ca59cf081b9d6   VSP8200.4.0.0.0_mib.txt
897303242c30fd944d435a4517f1b3f5   VSP8200.4.0.0.0_mib.zip
2fbd5eab1c450d1f5feae865b9e02baf   VSP8200.4.0.0.0_modules.tgz
a9d6d18a979b233076d2d3de0e152fc5   VSP8200.4.0.0.0_OpenSource.zip
8ce39996a131de0b836db629b5362a8a   VSP8200.4.0.0.0_oss-notice.html
80bfe69d89c831543623aaad861f12aa   VSP8200.4.0.0.0.tgz
a63a1d911450ef2f034d3d55e576eca0   VSP8200.4.0.0.0.zip
62b457d69cedd44c21c395505dcf4a80   VSP8200v400_HELP_EDM_gzip.zip
```

Calculate the md5 checksum for the file on the switch:

```
Switch:1>ls *.tgz
-rw-r--r--  1 0       0        44015148 Dec  8 08:18  VSP8200.4.0.0.0.tgz
-rw-r--r--  1 0       0        44208471 Dec  8 08:19  VSP8200.4.0.1.0.tgz
Switch:1>md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.0.0.0.tgz) = 80bfe69d89c831543623aaad861f12aa
```

Calculating and verifying the md5 checksum for a file on a client workstation

Perform this procedure on a Unix or Linux machine to verify that the software files downloaded properly. Avaya provides the md5 checksum for each release on the Avaya Support website.

About this task

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

Procedure

1. Calculate the md5 checksum of the downloaded file:

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

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

2. Verify the md5 checksum of the software suite:

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

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

Example

The following example uses files from Avaya Virtual Services Platform 4000 Series but the same process applies to software files for all VSP switches.

Calculate the md5 checksum of the downloaded file:

```
$ /usr/bin/md5sum VSP4K.4.0.40.0.tgz

02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.0.40.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.0.40.0.zip

a04e7c7cef660bb412598574516c548f VSP4000v4040_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.0.40.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.0.40.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.0.40.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.0.40.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.0.40.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.0.40.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.0.40.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

Calculating the MD5 digest

Before you begin

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

About this task

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

> **❗ Important:**
>
> If the MD5 key file parameters change, you must remove the old file and create a new file.

Procedure

1. Log on to the switch to enter User EXEC mode.

2. Calculate the MD5 digest:

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

Example

```
Switch:1> enable
```

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

```
Switch:1# md5 password —a —f password.md5
```

Variable definitions

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

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:

Table continues…

Variable	Value
	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 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:
	``` Switch: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) ```
-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

About this task

Reset system functions to reset all statistics counters on the console port. Depending on your hardware platform, the console port displays as console or 10101.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Reset system functions:

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

Example

```
Switch:1> enable
```

Reset the statistics counters:

```
Switch:1# sys action reset counters

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

Variable definitions

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

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

Sourcing a configuration

About this task

The **source** cli command is intended for use with a switch that is running with a factory default configuration to quick load a pre-existing configuration from a file. If you source a configuration file to merge that configuration into a running configuration, it can result in operational configuration loss if the sourced configuration file contains any configuration that has dependencies on or conflicts with the running configuration.

Procedure

1. Enter Privileged EXEC mode:

    ```
    enable
    ```

2. Source a configuration:

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

Example

```
Switch:1> enable
```

Debug the script output:

```
Switch:1# source testing.cfg debug
```

Variable definitions

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

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 format: • a.b.c.d:<file> • /intflash/<file> <file> is a string. The path and <file> can use 1–99 characters.

Using the USB device

The following sections describe common procedures that you can use with the USB device.

🛈 **Important:**

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

Saving a file to an external USB device

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

✳ **Note:**

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

⚠ **Caution:**

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the file to an external USB device:

   a. To save the configuration file to an external USB device, enter:

   ```
   save config file WORD<1–99>
   ```

   b. To save the log file to an external USB device, enter:

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

Example

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

Switch:1#
```

```
Switch:1#save log file /usb/test.log

Save log to file /usb/test.log successful.
Save log to file /usb/test.log successful.
Switch:1#
```

Variable definitions

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

Variable	Value
config file *WORD<1-99>*	Specifies the software configuration device and configuration file name in one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
log file *WORD<1-99>*	Specifies the software configuration device and log file name in one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.

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

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

 Note:

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

 Caution:

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

Before you begin

- **Important:**

  Disable logging using the command: `no boot config logging`.
- You must have a USB storage device ready to use that is at least 2 GB. The switch supports USB 1 and 2.

About this task

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

The backup action can take up to 10 minutes.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Backup the internal flash to USB:

   ```
   backup intflash
   ```

3. Restore the data to the internal flash:

   ```
   restore intflash
   ```

Example

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

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

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

For file system /intflash:
         7252475904 total bytes on the filesystem
          990920704 used bytes on the filesystem
         6261555200 free bytes on the filesystem

For file system /usb:
         2021216256 total bytes on the filesystem
           12038144 used bytes on the filesystem
         2009178112 free bytes on the filesystem

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

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

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

Copying configuration and log files from a USB device to Intflash

Copy configuration and log files from an external USB device to the internal Flash memory.

⊛ **Note:**

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Copy configuration or log files from the USB device to Intflash:

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

Example

```
Switch:1#enable
Switch:1#copy /usb/test.cfg /intflash/test.cfg
```

Variable definitions

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

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

Displaying content of a USB file

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

⊛ **Note:**

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

⚠ **Caution:**

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display content of a USB file:

   `more WORD<1-99>`

Example

`Switch:1#enable`

`Switch:1#more /usb/test.cfg`

Variable definitions

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

Variable	Value
WORD<1–99>	Specifies the file name in the following format: • /usb/<file> The file name, including the directory structure, can include up to 99 characters.

Moving a file to or from a USB device

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

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

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Move a file to a safe location:

   a. To move a file from Intflash to a USB device:

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

   b. To move a file from a USB device to Intflash:

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

Example

```
Switch:1#enable
Switch:1#mv /intflash/test.cfg /usb/test.cfg

Switch:1#enable
Switch:1#mv /usb/test.cfg /intflash/test.cfg
```

Variable definitions

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

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

Deleting a file from a USB device

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

★ **Note:**

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

⚠ **Caution:**

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Delete a file from a USB device:

   `delete WORD<1-255>`

Example

```
Switch:1#enable

Switch:1#delete /usb/test.cfg
Are you sure (y/n) ? y
```

Variable definitions

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

Variable	Value
WORD<1–255>	Specifies the file name in the following format: • /usb/<file>

Basic administration procedures using EDM

The following section describes common procedures that you use while you configure and monitor the switch operations using Enterprise Device Manager (EDM).

Resetting the platform

About this task

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

Procedure

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

Showing the MTU for the system

About this task

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

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation pane, expand the **Configuration** > **Edit** folders.
3. Click **Chassis**.

4. Click on the **Chassis** tab.

5. Verify the selection for the MTU size.

Displaying storage use

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

2. Click **File System**.

3. Click the **Storage usage** tab

Device Info field descriptions

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

Name	Description
IntflashBytesUsed	Specifies the number of bytes used in internal flash memory.
IntflashBytesFree	Specifies the number of bytes available for use in internal flash memory.
IntflashNumFiles	Specifies the number of files in internal flash memory.
UsbBytesUsed	Specifies the number of bytes used in USB device.
UsbBytesFree	Specifies the number of bytes available for use in USB device.
UsbNumFiles	Specifies the number of files in USB device.

Displaying available storage space

About this task

Display information about the available space for storage devices on this system.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

2. Click **Chassis**.

3. Click the **Storage Usage** tab.

Storage Usage field descriptions

Use the data in the following table to use the **Storage Usage** tab.

Name	Description
IntflashBytesUsed	Specifies the number of bytes used in internal flash memory.
IntflashBytesFree	Specifies the number of bytes available for use in internal flash memory.
IntflashNumFiles	Specifies the number of files in internal flash memory.
UsbBytesUsed	Specifies the number of bytes used in USB device.
UsbBytesFree	Specifies the number of bytes available for use in USB device.
UsbNumFiles	Specifies the number of files in USB device.

Displaying internal flash file information

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
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
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 internal flash files

Display information about the files on the internal flash.

⊛ **Note:**

This tab does not appear on all hardware platforms.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Chassis**.
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.
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 USB file information

About this task

Display information about the files on a USB device to view general file information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
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 of the device.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Copying a file

About this task

Copy files on the internal flash.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
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 or stops the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

Saving the configuration

About this task

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

★ **Note:**

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

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **System** tab.

5. **(Optional)** Specify a filename in **ConfigFileName**.

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

6. In **ActionGroup1**, select **saveRuntimeConfig**.

7. Click **Apply**.

Chapter 5: System startup fundamentals

This section provides conceptual material on the boot sequence and boot processes of the switch. Review this content before you make changes to the configurable boot process options.

spbm-config-mode boot flag

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

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

> 🛈 **Important:**
>
> Whenever you change the **spbm-config-mode** boot flag, you should save the configuration and reboot the switch for the change to take effect.

For more information about this boot flag and Simplified vIST, see *Configuring IP Multicast Routing Protocols*.

nni-mstp boot config flag

The nni-mstp boot flag changes the default behavior of the MSTP on SPBM NNI ports. The Common and Internal Spanning Tree (CIST) is disabled automatically on the NNI, and the NNI ports can only be members of backbone VLANs (B-VLAN).

- During startup, if you have non-B-VLAN on SPBM NNI ports in your configuration file, the system sets the nni-mstp flag to true (if it was not already set to true) and enables MTSP on SPBM NNI ports, and all other configurations remain the same. Save your configuration file. If you do not save your configuration, you continue to see the following message on reboot:

```
Warning
Detected brouter and/or vlans other than BVLANs on NNI ports. Setting the boot config
flag nni-mstp to true. Saving configuration avoids repetition of this warning on
reboot.
```

> **Note:**
>
> When the nni-mstp flag is set to true, only MSTI 62 is disabled on the SPBM NNI ports. You can add the SPBM NNI ports to any VLAN.

- If you configure the nni-mstp boot configuration flag to false (default), the system checks to make sure that the SPBM NNI ports do not have brouter (IPv4 or IPv6) or non-SPBM VLANs configured. The nni-mstp flag is then set to false. Save your configuration file, and reboot the switch for the configuration change to take effect.

> **Note:**
>
> Ensure that all SPBM NNI ports in non-B-VLAN are removed prior to setting the nni-mstp flag to false.

Example: Setting nni-mstp to true

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch:1(config)#boot config flags nni-mstp
Warning: Please save the configuration and reboot the switch for this configuration to
take effect.
Switch:1(config)#
```

Boot sequence

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

The boot sequence consists of the following stages:

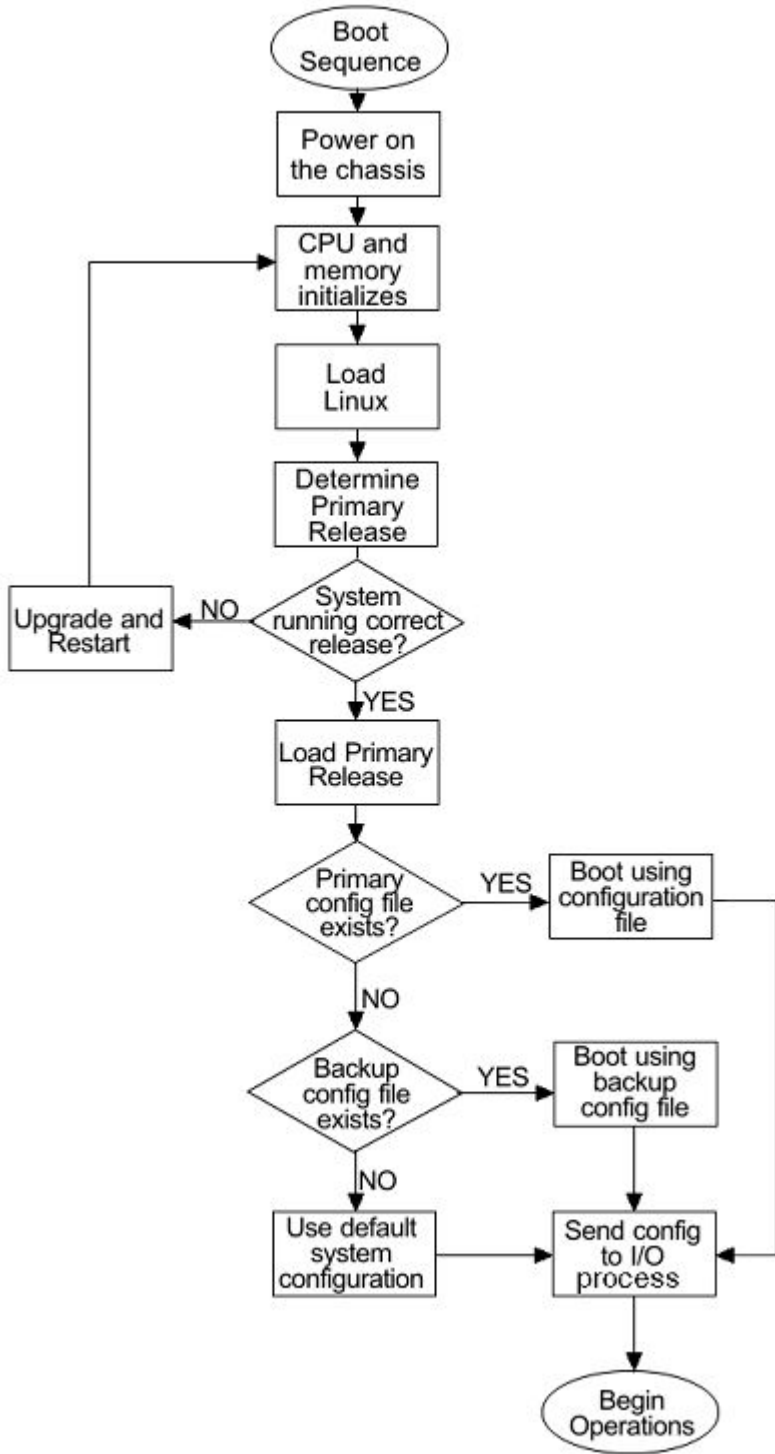The following figure shows a summary of the boot sequence.

Figure 1: Boot sequence

Stage 1: Loading Linux

The port contains a boot flash partition that stores the boot images, which include the boot loader, and the Linux kernel and applications. The boot flash partition contains two versions of the boot

image: a committed version (the primary release) and a backup version. A committed version is one that is marked as good (if you can start the system using that version). The system automatically uses the backup version if the system fails the first time you start with a new version.

Stage 2: Loading the primary release

The switch can install a maximum of six releases but can only load one of two—a primary (committed) release or a backup release.

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

After loading the primary release, the CPU and basic system devices such as the console port initializes. Depending on the hardware platform, the console port displays as console or 10101. At this stage, the I/O ports are not available; the system does not initialize the I/O ports until the port sends configuration data in stage 3.

Stage 3: Loading the configuration file

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

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

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

- Chassis configuration
- Port configuration
- Virtual LAN (VLAN) configuration
- Routing configuration
- IP address assignments
- Remote monitoring (RMON) configuration

The default switch configuration includes the following:

- A single, port-based default VLAN with a VLAN identification number of 1
- No interface assigned IP addresses
- Traffic priority for all ports configured to normal priority
- All ports as untagged ports
- Default communication protocol settings for the console port. For more information about these protocol settings, see System connections on page 56.

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 1: Configuration file statements

Sample statement	Action
`# software version    : 4.0.0.0`	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. The specified configuration file only gets loaded when the chassis starts. To load a new configuration file, you need to restart the system.

- Start the system without loading a configuration file, so that the system uses the factory default configuration. Bypassing the system configuration does not affect saved system configuration; the configuration simply does not load. This can be done by setting the factory defaults boot flag.

Run-time

After the switch 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 the switch

- 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. Depending on the hardware platform, the console port displays as console or 10101.

> **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 CLI using the `boot config flags` command. For information on system flags and their configuration, see

> **✳ Note:**
>
> The ipv6-mode flag does not apply to all hardware models.

Table 2: Boot config flags

CLI flag	Restart
`block-snmp`	No
`debug-config`	Yes
`debugmode`	Yes
`dvr-leaf-mode`	Yes
`enhancedsecure-mode`	Yes
`factorydefaults`	Yes
`flow-control-mode`	Yes
`ftpd`	No
`hsecure`	Yes
`ipv6-mode`	Yes
`logging`	No
`nni-mstp`	Yes
`reboot`	No
`rlogind`	No
`spanning-tree-mode`	Yes
`spbm-config-mode`	Yes
`sshd`	No
`telnetd`	No
`tftpd`	No
`trace-logging`	No
`urpf-mode`	Yes
`verify-config`	Yes
`vrf-scaling`	Yes
`vxlan-gw-full-interworking-mode`	Yes

System connections

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

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

To use the console port, you need a terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software. Depending on the hardware platform, the console port displays as console or 10101.

Client and server support

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

For active CLI clients, users initiate a client connection from the switch to another device.

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

Clients

IPv4 support:

The switch supports the following active CLI clients using IPv4:

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

The switch supports the following non active client using IPv4:

- Network Time Protocol (NTP)

IPv4 and IPv6 support:

The switch supports the following active CLI clients using IPv4.

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

> **Note:**
>
> Both FTP and TFTP clients are supported by the switch. The switch does not launch FTP and TFTP servers explicitly as a separate command; you can launch them through the CLI `copy` command. If you have configured the username through the **`boot config host`** command, the FTP client is used to transfer files to and from the switch using the CLI `copy` command; If you have not configured the username, the TFTP client is used to transfer files to and from the switch using the CLI `copy` command.
>
> Configuring the `boot config flags ftpd` or `boot config flags tftpd` enables the FTP or TFTP Servers on the switch.

The switch supports the following non active clients using IPv4 and IPv6:

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

Servers

IPv4 and IPv6 support:

The switch supports the following servers using IPv4:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- remote shell (rsh)
- rlogin
- Secure Copy (SCP)
- Secure File Transfer Protocol (SFTP)
- Secure Shell version 2 (SSHv2)
- Telnet
- Trivial File Transfer Protocol (TFTP)

Chapter 6: Boot parameter configuration using the CLI

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

Modifying the boot sequence

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ```
   boot config flags factorydefaults
   ```

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

   ```
   no boot config flags factorydefaults
   ```

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

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1# boot config flags factorydefaults
```

Configuring the remote host logon

Before you begin

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

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Define conditions for the remote host logon:

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

3. Save the changed configuration.

Example

```
Switch:1> enable
```

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

Enable console tftp/tftpd debug messages:

```
Switch:1# boot config host tftp-debug
```

```
Switch:1# save config
```

Enabling remote access services

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

Before you begin

- If you enable the rlogind flag, you must configure an access policy to specify the name of the user who can access the switch. For more information about access policies, see *Configuring Security*.

About this task

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), remote login (rlogin), Secure Shell version 2 (SSHv2), and Telnet server support IPv4 addresses.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enable the access service:

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

3. Save the configuration.

Example

Enable the access service to SSHv2:

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

Variable definitions

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

Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.
debug-config [console] | [file]	Enables you to debug the configuration file during loading configuration at system boot up. The default is disabled. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots.
	The options are:
	• debug-config [console]—Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file.
	• debug-config [file]— Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug config output to /intflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to /intflash/

Table continues…

Variable	Value
	debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.
debugmode	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging earlier on specified port. It only works on console connection. By default, it is disabled.
	❗ **Important:**
	Do not change this parameter unless directed by technical support.
dvr-leaf-mode	Enables an SPB node to be configured as a DvR Leaf.
	A node that has this flag set cannot be configured as a DvR Controller.
	Use the no or the default operator to disable this flag.
	The boot flag is disabled by default.
	For information on DvR, see *Configuring IPv4 Routing*.
enhancedsecure-mode {jitc | non-jitc}	Enables enhanced secure mode in either the JITC or non-JITC sub-modes.
	✳ **Note:**
	It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode, because the JITC sub-mode is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting.
	When you enable enhanced secure mode in either the JITC or non-JITC sub-modes, the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.

Table continues…

Variable	Value
flow-control-mode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames. The default is disabled.
ftpd	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the tftpd flag is disabled.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • The password must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 numbers, and 2 special characters. • Aging time • Failed login attempt limitation 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.
ipv6–mode	Enables IPv6 mode on the swtich. This parameter does not apply to all hardware platforms.
logging	Activates 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.

Table continues…

Variable	Value
	The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
nni-mstp	Enables MSTP, and allows non SPBM B-VLAN configuration on SPBM NNI ports.The default is disabled.
	⊛ **Note:**
	Spanning Tree is disabled on all SPBM NNIs.
	You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN.
	For information on releases that support the nni-mstp boot flag see *Release Notes*.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated.
	❗ **Important:**
	Do not change this parameter unless directed by technical support.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
spbm-config-mode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.
	Use the no operator so that you can configure PIM and IGMP.
	The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.
sshd	Activates or disables the SSHv2 server service. The default value is disabled.
telnetd	Activates or disables the Telnet server service. The default is disabled.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
trace-logging	Activates or disables the creation of trace logs. The default value is disabled.

Table continues…

Variable	Value
	❗ Important:
	Do not change this parameter unless directed by technical support.
urpf-mode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you configure it on a port or VLAN. The default is disabled.
verify-config	Activates syntax checking of the configuration file. The default is enabled.
	• Primary config behavior: When the verifyconfig flag is enabled, the primary config file is pre-checked for syntax errors. If the system finds an error, the primary config file is not loaded, instead the system loads the backup config file.
	If the verify-config flag is disabled, the system does not pre-check syntax errors. When the verify-config flag is disabled, the system ignores any lines with errors during loading of the primary config file. If the primary config file is not present or cannot be found, the system tries to load the backup file.
	• Backup config behavior: If the system loads the backup config file, the system does not check the backup file for syntax errors. It does not matter if the verify-config flag is disabled or enabled. With the backup config file, the system ignores any lines with errors during the loading of the backup config file.
	If no backup config file exists, the system defaults to factory defaults.
	It is recommended that you disable the verify-config flag.
vrf-scaling	Increases the maximum number of VRFs and Layer 3 VSNs that the switch supports. This flag is disabled by default.
	❗ Important:
	If you enable both this flag and the spbm-config-mode flag, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see *Release Notes*.

Table continues…

Variable	Value
vxlan-gw-full-interworking-mode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST. By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag. The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments. For more information about feature support, see *Configuring VLANs, Spanning Tree, and NLB*.

Changing the primary or secondary boot configuration files

About this task

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

Configure the primary boot choices.

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Change the primary boot choice:

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

3. Save the changed configuration.

4. Restart the switch.

Example

```
Switch:1> enable
Switch:1# configure terminal
```

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

```
Switch:1(config)# boot config choice primary config-file /intflash/
config.cfg
Switch:1(config)# save config
Switch:1(config)# reset
```

Variable definitions

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

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 format: • a.b.c.d:<file> • /usb/<file> • /intflash/<file> To set this option to the default value, use the default operator with the command.

Configuring boot flags

Before you begin

- If you enable the hsecure flag, you cannot enable the flags for the Web server or SSH password-authentication.

  🛈 **Important:**

  After you change certain configuration parameters using the **boot config flags** command, you must save the changes to the configuration file.

About this task

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

⊛ **Note:**

The ipv6-mode flag does not apply to all hardware models.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Enable boot flags:

```
boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode <jitc|non-jitc> |dvr-leaf-mode|factorydefaults|
flow-control-mode|ftpd|hsecure|ipv6-mode|logging|nni-mstp|reboot|
rlogind|spanning-tree-mode <mstp|rstp>|spbm-config-mode|sshd|
telnetd|tftpd|trace-logging|urpf-mode|verify-config|vrf-scaling|
vxlan-gw-full-interworking-mode
```

3. Disable boot flags:

```
no boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode|dvr-leaf-mode|factorydefaults|flow-control-mode|
ftpd|hsecure|ipv6-mode|logging|nni-mstp|reboot|rlogind|spanning-
tree-mode|spbm-config-mode|sshd|telnetd|tftpd|trace-logging|urpf-
mode|verify-config|vrf-scaling|vxlan-gw-full-interworking-mode
```

4. Configure the boot flag to the default value:

```
default boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode|dvr-leaf-mode|factorydefaults|flow-control-mode|
ftpd|hsecure|ipv6-mode|logging|nni-mstp|reboot|rlogind|spanning-
tree-mode|spbm-config-mode|sshd|telnetd|tftpd|trace-logging|urpf-
mode|verify-config|vrf-scaling|vxlan-gw-full-interworking-mode
```

5. Save the changed configuration.

6. Restart the switch.

Example

```
Switch:1> enable
```

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

Activate High Secure mode:

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

```
Switch:1(config)# save config
```

```
Switch:1(config)# reset
```

Variable definitions

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

Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.
debug-config [console] | [file]	Enables you to debug the configuration file during loading configuration at system boot up. The default is disabled. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots. The options are: • debug-config [console]—Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file. • debug-config [file]— Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug config output to /intflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to /intflash/debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.
debugmode	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging earlier on specified port. It only works on console connection. By default, it is disabled. **❗ Important:** Do not change this parameter unless directed by technical support.
dvr-leaf-mode	Enables an SPB node to be configured as a DvR Leaf. A node that has this flag set cannot be configured as a DvR Controller. Use the no or the default operator to disable this flag. The boot flag is disabled by default. For information on DvR, see *Configuring IPv4 Routing*.

Table continues…

Variable	Value
enhancedsecure-mode {jitc | non-jitc}	Enables enhanced secure mode in either the JITC or non-JITC sub-modes. ✱ **Note:** It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode, because the JITC sub-mode is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting. When you enable enhanced secure mode in either the JITC or non-JITC sub-modes, the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
flow-control-mode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames. The default is disabled.
ftpd	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the tftpd flag is disabled.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • The password must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 numbers, and 2 special characters. • Aging time • Failed login attempt limitation The default value is disabled. If you enable High Secure mode, you must restart the switch to enforce

Table continues…

Variable	Value
	secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.
ipv6–mode	Enables IPv6 mode on the swtich. This parameter does not apply to all hardware platforms.
logging	Activates 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.
nni-mstp	Enables MSTP, and allows non SPBM B-VLAN configuration on SPBM NNI ports.The default is disabled. ✳ **Note:** Spanning Tree is disabled on all SPBM NNIs. You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN. For information on releases that support the nni-mstp boot flag see *Release Notes*.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated. ❗ **Important:** Do not change this parameter unless directed by technical support.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode.

Table continues…

Variable	Value
	The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
spbm-config-mode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. Use the no operator so that you can configure PIM and IGMP. The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.
sshd	Activates or disables the SSHv2 server service. The default value is disabled.
telnetd	Activates or disables the Telnet server service. The default is disabled.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
trace-logging	Activates or disables the creation of trace logs. The default value is disabled. **❗ Important:** Do not change this parameter unless directed by technical support.
urpf-mode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you configure it on a port or VLAN. The default is disabled.
verify-config	Activates syntax checking of the configuration file. The default is enabled. • Primary config behavior: When the verifyconfig flag is enabled, the primary config file is pre-checked for syntax errors. If the system finds an error, the primary config file is not loaded, instead the system loads the backup config file. If the verify-config flag is disabled, the system does not pre-check syntax errors. When the verify-config flag is disabled, the system ignores any lines with errors during loading of the primary config file. If the primary config file is not present or cannot be found, the system tries to load the backup file. • Backup config behavior: If the system loads the backup config file, the system does not check the

Table continues…

Variable	Value
	backup file for syntax errors. It does not matter if the verify-config flag is disabled or enabled. With the backup config file, the system ignores any lines with errors during the loading of the backup config file. If no backup config file exists, the system defaults to factory defaults. It is recommended that you disable the verify-config flag.
vrf-scaling	Increases the maximum number of VRFs and Layer 3 VSNs that the switch supports. This flag is disabled by default. 🛈 **Important:** If you enable both this flag and the spbm-config-mode flag, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see *Release Notes*.
vxlan-gw-full-interworking-mode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST. By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag. The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments. For more information about feature support, see *Configuring VLANs, Spanning Tree, and NLB*.

Configuring serial port devices

About this task

Configure the serial port devices to define connection settings for the console port. Depending on your hardware platform the console port displays as console or 10101.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   
   configure terminal
   ```

Comments on this document? infodev@avaya.com

2. **(Optional)** Change the baud rate for the port:

   `boot config sio console baud <9600-115200>`

3. Save the changed configuration.

4. Restart the switch.

Example

`Switch:1> enable`

`Switch:1# config terminal`

Configure the baud rate to 9600 for the port:

`Switch: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.

Variable	Value
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 configuration

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View the configuration:

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

Example

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

```
Switch:1>enable

Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch:1#(config)#show boot config running-config
#
#Thu Mar 20 15:12:01 2014 UTC
#
boot config flags ftpd
boot config flags rlogind
boot config flags sshd
boot config flags telnetd
boot config flags tftpd
no boot config flags verify-config
boot config choice primary backup-config-file "/intflash/config.cfg"
```

Variable definitions

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

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

Chapter 7: Run-time process management using CLI

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

Configuring the date

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Log on as rwa to perform this procedure.

3. Configure the date:

   ```
   clock set <MMddyyyyhhmmss>
   ```

Example

```
Switch:1> enable

Switch:1# clock set 19042014063030
```

Variable definitions

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

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

Configuring the time zone

About this task

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

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

> ❗ **Important:**
>
> In October 2014, the government of Russia moved Moscow from UTC+4 into the UTC+3 time zone with no daylight savings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

3. Save the changed configuration.

Example

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

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

Variable definitions

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

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` 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.

Table continues…

Variable	Value
	To see a list of options, enter `clock time-zone` at the command prompt without variables.

Configuring the run-time environment

About this task

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

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Change the login prompt:

   `login-message WORD<1-1513>`

3. Change the password prompt:

   `passwordprompt WORD<1-1510>`

4. Configure the number of supported rlogin sessions:

   `max-logins <0-8>`

5. Configure the number of supported inbound Telnet sessions:

   `telnet-access sessions <0-8>`

6. Configure the idle timeout period before automatic logoff for CLI and Telnet sessions:

   `cli timeout <30-65535>`

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

   `terminal length <8-64>`

8. Configure scrolling for the output display:

   `terminal more <disable|enable>`

Example

`Switch:1> enable`

`Switch:# configure terminal`

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

`Switch:(config)# default login-message`

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

```
Switch:(config)# default passwordprompt
```

Configure the allowable number of inbound remote CLI logon sessions:

```
Switch:(config)# max-logins 5
```

Configure the allowable number of inbound Telnet sessions:

```
Switch:(config)# telnet-access sessions 8
```

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

```
Switch:(config)# cli timeout 900
```

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

```
Switch:(config)# terminal length 30
```

Configure scrolling for the output display:

```
Switch:(config)# terminal more disable
```

Variable definitions

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

Variable	Value
WORD<1-1513>	Changes the CLI 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.

Variable	Value
WORD<1-1510>	Changes the CLI 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.

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

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

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.

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

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

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

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Create a custom banner:

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

Example

```
Switch:1> enable
```

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

Activate the use of the default banner:

```
Switch:1(config)# banner static
```

Variable definitions

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

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

Configuring the message-of-the-day

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Create the message-of-the-day:

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

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

```
banner displaymotd
```

Example

```
Switch:1> enable
```

```
Switch: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.):

```
Switch:1(config)# banner motd "Unauthorized access is forbidden"
```

Enable the custom message-of-the-day:

```
Switch:1(config)# banner displaymotd
```

Variable definitions

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

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 CLI logging

About this task

Use CLI logging to track all CLI commands executed and for fault management purposes. The CLI 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 CLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable CLI logging:

   ```
   clilog enable
   ```

3. Disable CLI logging:

   ```
   no clilog enable
   ```

4. Ensure that the configuration is correct:

   ```
   show clilog
   ```

5. View the CLI log:

```
show logging file module clilog
```

6. View the CLI log.

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#clilog enable
```

Variable definitions

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

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

Configuring system parameters

About this task

Configure individual system-level switch parameters to configure global options for the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Change the system name:

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

3. Enable support for Jumbo frames:

```
sys mtu 1950
```

OR

```
sys mtu 9600
```

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

```
udp checksum
```

Example

```
Switch:1> enable
```

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

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

```
Switch:1(config)# sys name Floor3Lab2
```

Variable definitions

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

Variable	Value
mtu *<1522|9600>*	Activates Jumbo frame support for the data path. The value can be either 1522, 1950 (default), or 9600 bytes. 1950 or 9600 bytes activate Jumbo frame support.
name *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).
clipId-topology-ip	Set the topology ip from the available CLIP. *WORD<1-256>*Specifies the Circuitless IP interface id.
force-msg	Adds forced message control pattern. *WORD<4–4>* Enter force message pattern.
force-topology-ip-flag	Flag set to force choice of topology flag. *enable*
msg-control	Enbales system message control feature.

Configuring system message control

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure system message control action:

   ```
   sys msg-control action <both|send-trap|suppress-msg>
   ```

3. Configure the maximum number of messages:

```
        sys msg-control max-msg-num <2-500>
```

4. Configure the interval:

```
        sys msg-control control-interval <1-30>
```

5. Enable message control:

```
        sys msg-control
```

Example

```
Switch:1> enable
```

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

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

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

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

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

Configure the message control interval in minutes:

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

Enable message control:

```
Switch:1(config)# sys msg-control
```

Variable definitions

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

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

Extending system message control

About this task

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the force message control option:

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

Example

```
Switch:1> enable
```

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

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

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

Variable definitions

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

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

The following sections provide information for chassis operations such as hardware and software compatibility.

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.

Management port

The management port is a 10/100/1000 Mb/s Ethernet port that you can use for an out-of-band management connection to the switch.

To remotely access the switch using the management port, you have to configure an IP address for the management port.

> ✱ **Note:**
>
> Not all hardware platforms include a dedicated, physical management interface. For more information about supported interfaces, see your hardware documentation.

Management Router VRF

The switch has a separate VRF called Management Router (MgmtRouter) reserved for OAM (mgmt) port. The configured IP subnet has to be globally unique because the management protocols, for example, SNMP, Telnet, and FTP, can go through in-band or out-of-band ports. The VRF ID for the Management Router is 512.

The switch never switches or routes transit packets between the Management Router VRF port and the Global Router VRF, or between the Management Router VRF and other VRF ports.

The switch honors the VRF of the ingress packet; however, in no circumstance does the switch allow routing between the Management VRF and Global Router VRF. The switch does not support the configuration if you have an out-of-band management network with access to the same networks present in the GRT routing table.

Non-virtualized client management applications

It is recommended that you do not define a default route in the Management Router VRF. A route originating from the switch and used for non-virtualized client management applications, such as Telnet, Secure Shell (SSH), and FTP will always match a default route defined in the Management Router VRF.

If you want out-of-band management, define a specific static route in the Management Router VRF to the IP subnet where your management application resides. When you specify a static route in the Management Router VRF, it enables the client management applications originating from the switch to perform out-of-band management without affecting in-band management. This enables in-band management applications to operate in the Global Router VRF.

Non-virtualized client management applications originating from the switch, such as Telnet, SSH, and FTP, follow the behavior listed below:

1. Look at the Management Router VRF route table
2. If no route is found, the applications will proceed to look in the Global Router VRF table

Non-virtualized client management applications include:

- DHCP Relay
- DNS
- FTP client with the `copy` command
- NTP
- rlogin
- RADIUS authentication and accounting
- SSH
- SNMP clients in the form of traps
- SYSLOG
- TACACS+
- Telnet
- TFTP client

For management applications that originate outside the switch, the initial incoming packets establish a VRF context that limits the return path to the same VRF context.

Virtualized management applications

Virtualized management applications, such as ping and traceroute, operate using the specified VRF context. To operate ping or traceroute you must specify the desired VRF context. If not specified, ping defaults to the Global Router VRF. For example, if you want to ping a device through the out-of-band management port you must select the Management Router VRF.

```
Switch:1(config)#ping 192.0.2.1 vrf MgmtRouter
192.0.2.1 is alive
```

Entity MIB – Physical Table

The Entity MIB – Physical Table assists in the discovery of functional components on the switch. The Entity MIB – Physical Table supports a physical interface table that includes information about the chassis, power supply, fan, I/O cards, console, and management port.

Some hardware platforms support removable interface modules while others offer a fixed configuration. The names used for these modules can vary depending on the hardware platform.

The following table identifies the entity index range for the switch components.

Component	Entity index range
Chassis	1
Power supply slot	2 to 7
Fan tray and fan slot	8 to 15
I/O slot	16 to 35
I/O card or module	36 to 55
Console port	56
Management port	57
Power supply	68 to 73
Fan tray	74 to 81
Fan module	82 to 105

For more information about Entity MIB – Physical Table, see

Software lock-up detection

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

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

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

The CPU logs detail about suspended tasks in the log file. For additional information about log files, see *Monitoring Performance*.

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. The switch supports Ethernet frames as large as 9600 bytes, compared to the standard 1518 bytes, to transmit large amounts of data efficiently and minimize the task load on a server CPU.

Tagged VLAN support

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

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

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

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

😶 **Note:**

Not all hardware platforms support Auto-Negotiation. For more information, see your hardware documentation.

Default Auto-Negotiation behavior varies depending on the hardware platform. For information about feature support, see *Release Notes*.

You should configure Auto-Negotiation as shown in the following table, where A and B are two Ethernet devices.

❗ **Important:**

If Auto-Negotiation is disabled, the 8424GT ESM, the 8424XT ESM and the VSP 7254XTQ switch do not support half-duplex.

Table 3: Recommended Auto-Negotiation configuration on 10/100/1000BASE-TX ports

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

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

* **Note:**

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

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

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

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

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

40 GbE Auto-Negotiation recommendation

Auto-Negotiation should be enabled in 40 GbE ports when using 40GbCR4 (copper Direct Attached Cables - DACs) pluggable modules as Clause 73 of the 40 GbE standard lists it as mandatory. Though the links may come up in 40 GbE ports even without Auto-Negotiation, it is strongly recommended to always enable Auto-Negotiation. Otherwise, there might be link instability or FCS errors.

SynOptics Network Management Protocol

The switch supports 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.

Channelization

Channelization allows you to configure 40 Gbps QSFP+ ports to operate as four 10 Gigabit Ethernet ports. You can use QSFP+ to four SFP+ breakout cables or QSFP+ transceivers with fiber breakout cables to connect the 10 Gigabit Ethernet ports to other servers, storage, and switches.

By default, the ports are not channelized, which means that the 40 Gbps QSFP+ ports operate as 40 Gigabit Ethernet ports. You can enable or disable channelization on a port.

For the number of 40 Gbps ports on your switch that support channelization, see your hardware documentation.

If your product supports channelization and you enable or disable channelization on a port, the port QoS configuration resets to default values. For information about configuring QoS values, see *Configuring QoS and ACL-Based Traffic Filtering*.

Note that when you use channelized ports in an SMLT configuration, you will not see the channelized ports displayed properly when you show MLT information for the remote port member if a release earlier than 4.2.0.0 is running on the remote switch.

When a port is channelized, only use break out cables (DAC or Fiber) in it. Otherwise, the link behavior can be unpredictable because it can result in mismatched link status between link partners, which can further lead to network issues. Also avoid the use of break out cables in non-channelized ports because this can result in mismatched link status between link partners, which can lead to network issues.

Feature interaction with channelization

Software features operate on channelized ports. When an interface is dechannelized, the interface cleans up all the channels.

If a feature operates on channel 1/1/1 and 1/1/2, and the circuit is dechannelized, the 1/1/1 configuration is saved and the commands are configured on 1/1. The configuration on 1/1/2 is deleted.

IEEE 802.3X Pause frame transmit

The switch uses MAC pause frames to provide congestion relief on full-duplex interfaces.

Overview

When congestion occurs on an egress port, the system can send pause frames to the offending devices to stop the packet flow. The system uses flow control if the rate at which one or more ports receives packets is greater than the rate at which the switch transmits packets.

The switch generates pause frames to tell the sending device to stop sending additional packets for a specified time period. After the time period expires, the sending device can resume sending packets. During the specified time period, if the switch determines the congestion is reduced, it can send pause frames to the sending device to instruct it to begin sending packets immediately.

Flow control mode and pause frames

If you enable flow control mode globally, the switch drops packets on ingress when congestion occurs. If the switch is not in flow control mode, it drops packets at egress when congestion occurs.

Configure an interface to send pause frames when congestion occurs to alleviate packet drops due to flow control mode.

Auto-Negotiation

Interfaces that support auto-negotiation advertise and exchange their flow control capability to agree on a pause frame configuration. IEEE 802.3 annex 28b defines the auto-negotiation ability fields and the pause resolution. The switch advertises only two capabilities. The following table shows the software bit settings based on the flow control configuration.

★ **Note:**

Not all interfaces support Auto-Negotiation. For more information, see your hardware documentation.

Table 4: Advertised abilities

Interface configuration	Pause	ASM	Capability advertised
Flow control enabled	1	0	Symmetric pause
Flow control disabled	1	1	Both Symmetric pause and asymmetric pause

The following tables identifies the pause resolution.

Table 5: Pause resolution

Local device pause	Local device ASM	Peer device pause	Peer device ASM	Local device resolution	Peer device resolution
0	0	Do not care	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	0	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	1	0	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	1	1	Enable pause transmit. Disable pause receive.	Disable pause transmit. Enable pause receive.
1	0	0	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
1	Do not care	1	Do not care	Enable pause transmit and receive.	Enable pause transmit and receive.
1	1	0	0	Disable pause transmit and receive.	Disable pause transmit and receive.
1	1	0	1	Disable pause transmit. Enable pause receive.	Enable pause transmit. Disable pause receive.

The following list identifies the type of interfaces that support auto-negotiated flow control:

- 10 Mbps/100 Mbps/1 Gbps copper
- 100 Mbps/1 Gbps/10 Gbps copper
- 1 Gbps fiber (in both SFP and SFP+ ports)

Auto MDIX

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

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

CANA

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

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

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

❗ Important:

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

❗ Important:

CANA is supported on the 8424XT ESM, the 8424XTQ ESM, the 8424GT ESM and the VSP 7254XTQ.

The switches support only full-duplex. Half-duplex is not supported.

Chassis operations configuration using the CLI

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

Enabling jumbo frames

About this task

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

Procedure

1. Enter Global Configuration mode:

    ```
    enable
    ```

```
configure terminal
```

2. Enable jumbo frames:

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

Example

```
Switch:1> enable
```

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

Enable jumbo frames to 9600 bytes:

```
Switch:1#(config)# sys mtu 9600
```

Variable definitions

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

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

Configuring port lock

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enable port lock globally:

```
portlock enable
```

3. Log on to GigabitEthernet Interface Configuration mode:

```
interface gigabitethernet {slot/port[/sub-port][-slot/port[/sub-
port]][,...]}
```

4. Lock a port:

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

Example

```
Switch:1> enable
```

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

Log on to GigabitEthernet Interface Configuration mode:

```
Switch:1(config)# interface GigabitEthernet 1/1
```

Unlock port 1/14:

```
Switch:1(config-if)# no lock port 1/14 enable
```

Variable definitions

Use the data in the following table to use the **interface gigabitethernet** and **lock port** commands.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
	For the `lock port` command, use the no form of this command to unlock a port: `no lock port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}`

Configuring SONMP

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. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Disable SONMP:

   ```
   no autotopology
   ```

3. Enable SONMP:

```
        autotopology
```

Example

```
Switch:1> enable
```

```
Switch:1 configure terminal
```

Disable SONMP:

```
Switch:1(config)# no autotopology
```

Viewing the topology message status

About this task

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

Procedure

1. Log on to the switch to enter User EXEC mode.

2. Show the contents of the topology table:

   ```
   show autotopology nmm-table
   ```

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

Example

> ⊛ **Note:**
>
> In the following example, the column "ChassisType" uses a generic name. When you use the **show autotopology nmm-table**, your switch displays the actual chassis type.

```
Switch:1(config)#show autotopology nmm-table
================================================================================
                                Topology Table
================================================================================
Local                                                                      Rem
Port      IpAddress       SegmentId MacAddress    ChassisType         BT LS CS  Port
--------------------------------------------------------------------------------
0/0       10.139.43.81    0x000000  0030ab707a00  ChassisType 1       12 Yes HtBt  0/0
1/1       10.139.43.81    0x000000  0050ea268800  ChassisType 2       12 Yes HtBt  1/50
1/42      10.139.43.81    0x000000  070ab307aa00  ChassisType 3       12 Yes HtBt  1/1
2/1       10.139.43.81    0x000000  0030ab57ab00  ChassisType 4       12 Yes HtBt  1/49
2/2       10.139.43.81    0x000000  0030ab307af0  ChassisType 5       12 Yes HtBt  1/50
2/41      10.139.43.81    0x000000  00e0ba327c00  ChassisType 6       12 Yes HtBt  2/1
2/42/1    10.139.43.81    0x000000  0050eb127400  ChassisType 7       12 Yes HtBt  1/2
```

> ⊛ **Note:**
>
> When a peer switch is running an older software version that does not include support for SONMP hello messages with channelization information, it can only show the slot/port. It cannot show the sub-port.

Job aid

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

Table 6: 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. The switch 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.

Associating a port to a VRF instance

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

Before you begin

• The VRF instance must exist. For more information about the creation of VRFs, see *Configuring IPv4 Routing*.

About this task

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

Procedure

1. Enter Interface Configuration mode:

   `enable`

```
configure terminal

interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-
port]][,...]} or interface vlan <1-4059>
```

> ⊛ **Note:**
>
> If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Associate a VRF instance with a port:

```
vrf <WORD 1-16>
```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# interface gigabitethernet 1/12

Switch:1(config-if)# vrf red
```

Configuring an IP address for the management port

Configure an IP address for the management port so that you can remotely access the device using the out-of-band (OOB) management port. The management port runs on a dedicated VRF.

The configured IP subnet has to be globally unique because the management protocols can go through in-band (Global Router) or out-of-band ports (Management VRF).

> ⊛ **Note:**
>
> This procedure only applies to hardware with a dedicated physical management interface.

Before you begin

- Do not configure a default route in the Management VRF.
- If you want out-of-band management, define a specific static route in the Management Router VRF to the IP subnet where your management application resides.
- If you initiate an FTP session from a client device behind a firewall, you should set FTP to passive mode.
- The switch gives priority to out-of-band management when there is reachability from both in-band and out-of-band. To avoid a potential conflict, do not configure any overlapping between in-band and out-of-band networks.

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

```
enable

configure terminal

interface mgmtEthernet mgmt
```

2. Configure the IP address and mask for the management port:

   `ip address {<A.B.C.D/X> | <A.B.C.D> <A.B.C.D>}`

3. Configure an IPv6 address and prefix length for the management port:

   `ipv6 interface address WORD<0-255>`

4. Show the complete network management information:

   `show interface mgmtEthernet`

5. Show the management interface packet/link errors:

   `show interface mgmtEthernet error`

6. Show the management interface statistics information:

   `show interface mgmtEthernet statistics`

Example

Configure the IP address for the management port:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface mgmtethernet mgmt
Switch:1(config-if)#ip address 192.0.2.31 255.255.255.0
```

Variable definitions

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

Variable	Value
*{<A.B.C.D/X>	<A.B.C.D> <A.B.C.D>}*	Specifies the IP address followed by the subnet mask.

Use the data in the following table to use the **ipv6 interface address** command.

Variable	Value
WORD<0-255>	Specifies the IPv6 address and prefix length.

Configuring Ethernet ports with Autonegotiation

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

The default is enabled for VSP 4000 Series and VSP 8000 Series but disabled for VSP 7200 Series.

About this task

❗ Important:

- When you use 1 Gigabit Ethernet SFP transceivers on VSP 7254XSQ, the software disables auto-negotiation on the port:

  - If you use 1 Gbps fiber SFP transceivers, the remote end must also have auto-negotiation disabled.

  - If you use 1 Gbps copper SFP transceivers, the remote end must have auto-negotiation enabled. If not, the link will not be established.

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

- The software requires the same auto-negotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down. Ensure the auto-negotiation settings between local ports and their remote link partners match before you upgrade the software.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   `enable`

   `configure terminal`

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

   ✳ Note:

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

2. Enable Autonegotiation:

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

3. Disable Autonegotiation:

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

Example

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

Variable definitions

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

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port or ports that you want to configure.
enable	Enables auto-negotiation for the port or other ports of the module.
	The default is enabled for VSP 4000 Series and VSP 8000 Series but disabled for VSP 7200 Series.

Configuring IEEE 802.3X Pause frame transmit

Configure IEEE 802.3X Pause frame transmit to eliminate or minimize packet loss.

About this task

By default, flow control mode is disabled. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames.

By default, an interface does not send pause frames.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enable flow control mode:

   `boot config flags flow-control-mode`

3. Save the configuration.

4. Exit Privileged EXEC mode:

   `exit`

5. Reboot the chassis.

   `boot`

6. Enter GigabitEthernet Interface Configuration mode:

   `enable`

   `configure terminal`

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

   ⭐ **Note:**

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

7. Configure the interface to generate pause frames:

```
tx-flow-control [enable]
```

8. **(Optional)** Configure other interfaces to generate pause frames:

```
tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]]
[,...]} enable
```

9. Verify the boot flag configuration:

```
show boot config flags
```

10. Verify the interface configuration:

```
show interfaces gigabitEthernet l1-config {slot/port[/sub-port] [-
slot/port[/sub-port]] [,...]}
```

11. View the pause-frame packet count:

```
show interfaces gigabitEthernet statistics {slot/port[/sub-port] [-
slot/port[/sub-port]] [,...]}
```

Example

Enable flow control on the system and configure slot 1, port 10 to send pause frames. Verify the configuration.

⊛ **Note:**

Slot and port information can differ depending on hardware platform. See your hardware documentation for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#boot config flags flow-control-mode
Warning: Please save the configuration and reboot the switch
        for this configuration to take effect.
Switch:1<config>#save config
CP-1: Save config to file /intflash/config.cfg successful.
CP-1: Save license to file /intflash/license.xml successful.
Switch:1<config>#exit
Switch:1#boot
Are you sure you want to re-boot the switch (y/n) ?y
```

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface gigabitethernet 1/10
Switch:1(config-if)#tx-flow-control enable
Switch:1(config-if)#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags dvr-leaf-mode false
flags enhancedsecure-mode false
flags factorydefaults false
flags flow-control-mode true
flags ftpd false
flags hsecure false
flags ipv6-mode false
```

```
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd false
flags telnetd true
flags tftpd false
flags trace-logging false
flags urpf-mode false
flags verify-config true
flags vrf-scaling false

flags vxlan-gw-full-interworking-mode false

Switch:1(config-if)#show interfaces gigabitEthernet l1-config 1/10
================================================================================
                                   Port Config L1
================================================================================
PORT    AUTO  CUSTOM AUTO NEGOTIATION    ADMIN      OPERATE    ADMIN        OPERATE
NUM     NEG.  ADVERTISEMENTS             DPLX  SPD  DPLX  SPD  TX-FLW-CTRL  TX-FLW-CTRL
--------------------------------------------------------------------------------
1/10    true Not Configured              full 10000    0       enable       enable
```

View the pause-frame packet count for slot 1, port 10.

```
Switch:1(config-if)#show interfaces gigabitEthernet statistics 1/10
====================================================================================
                                   Port Stats Interface
====================================================================================
PORT    IN              OUT             IN              OUT
NUM     OCTETS          OCTETS          PACKET          PACKET
------------------------------------------------------------------------------------
1/1     29964704384     22788614528     234106526       178034166

PORT    IN              OUT             IN              OUT             OUTLOSS
NUM     FLOWCTRL        FLOWCTRL        PFC             PFC             PACKETS
------------------------------------------------------------------------------------
1/1     0               11014           0               0               0
```

Variable definitions

Use the data in the following table to use the **tx-flow-control** command.

Variable	Value
enable	Configures the interface to send pause frames. By default, flow control is disabled.
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Use the data in the following table to use the **show interfaces gigabitEthernet l1-config** and **show interfaces gigabitEthernet statistics** commands.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Enabling channelization

Enable channelization on a port to configure it to operate as four channels, or ports.

🛈 **Important:**

Not all hardware platforms support the same port speeds or the channelization feature. For more information about feature support, see *Release Notes*.

About this task

✳ **Note:**

Enabling or disabling channelization resets the port QoS configuration to default values. For information about configuring QoS values, see *Configuring QoS and ACL-Based Traffic Filtering*.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ✳ **Note:**

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

2. Enable channelization on a port:

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

3. Display the status of the ports:

   ```
   show interfaces gigabitEthernet channelize [{slot/port[-slot/port]
   [,...]}]
   ```

   To display the details of the sub-ports, use:

```
show interfaces gigabitEthernet channelize detail [{slot/port/sub-
port[-slot/port/sub-port][,...]}]
```

4. **(Optional)** To disable channelization on a port, enter:

```
no channelize [port {slot/port[/sub-port] [-slot/port[/sub-port]]
[,...]}] enable
```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# interface gigabitethernet 2/1
Switch:1(config-if)# channelize enable
Enabling channelization on port 2/1. Subport 2/1/1 will inherit port 2/1 configuration.
Subports 2,3,4 will use default config. QSFP will be reset as removal and re-insert.
    NOTE: Modify QOS configurations on all subports as required.
Do you wish to continue (y/n) ? y
```

Display the port status:

```
Switch:1(config)# show interfaces gigabitEthernet channelize 2/2-2/4


================================================================================
                          Port Channelization
================================================================================
--------------------------------------------------------------------------------
PORT            ADMIN MODE     CHANNEL TYPE
--------------------------------------------------------------------------------
2/2             true           40G
2/3             false          40G
2/4             false          40G
```

The following is an example of how to disable channelization on a port:

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# interface gigabitethernet 2/2/1
Switch:1(config-if)# no channelize enable
```

Variable definitions

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

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring serial management port dropping

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

- modem power failure

- link disconnection

- loss of the carrier

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

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

For more information on enhanced secure mode, see Enabling enhanced secure mode on page 262.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ```
   sys security-console
   ```

Example

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

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

Controlling slot power

About this task

The `sys power slot` command is used to control slot power on an Avaya Virtual Services Platform 8400.

🛈 **Important:**

This command is only available for use with the Avaya Virtual Services Platform 8400.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure slot power:

   ```
   [no] sys power slot {slot[-slot][,...]}
   ```

Example

Enable power to Slot 1:

```
Switch:1 (config)# sys power slot 1
```

Disable power to Slot 1:

```
Switch:1 (config)# no sys power slot 1
```

Enable power to Slots 1 and 2:

```
Switch:1 (config)# sys power slot 1, 2
```

Disable power to Slots 1 and 2:

```
Switch:1 (config)# no sys power slot 1, 2
```

Variable definitions

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

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (1), a range of slots 1–3), or a series of slots (1,2,4).

Enabling or disabling the USB port

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

> ⓘ **Important:**
>
> Do not perform this procedure on a VSP 4850.
>
> The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first

used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

Before you begin

• The switch must be in Enhanced Secure mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the USB port:

   ```
   sys usb disable
   ```

3. Enable a previously disabled USB port:

   ```
   no sys usb disable
   ```

Chassis operations configuration using EDM

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

Editing system information

About this task

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

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **System** tab.

5. In the **sysContact** field, enter the contact information.

6. In the **sysName** field, enter the system name.

7. In the **sysLocation** field, enter the location information.

8. Click **Apply**.

System field descriptions

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

Name	Description
sysDescr	Shows the system assigned name and the software version.
sysUpTime	Shows the elapsed time since the system last started.
sysContact	Configures the contact information.
sysName	Configures the name of this device.
sysLocation	Configures the physical location of this device.
VirtualIpv6Addr	Specifies the virtual IPv6 address.
VirtualIpv6PrefixLength	Specifies the length of the virtual IPv6 address prefix (in bits).
DnsDomainName	Configures the default domain for querying the DNS server.
LastChange	Displays the time since the last configuration change.
LastVlanChange	Displays the time since the last VLAN change.
LastStatisticsReset	Displays the time since the statistics counters were last reset.
LastRunTimeConfigSave	Displays the last run-time configuration saved.
DefaultRuntimeConfigFileName	Displays the default Run-time configuration file directory name.
ConfigFileName	Specifies the name of a new configuration file.
ActionGroup1	Can be one of the following actions: • resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration • loadLicense—Loads a software license file to enable features
ActionGroup2	Specifies the following action: resetIstStatCounters—Resets the IST statistic counters
ActionGroup3	Can be the following action: • flushIpRouteTbl—flushes IP routes from the routing table

Table continues…

Name	Description
ActionGroup4	Can be the following action: • softReset—resets the device without running power-on tests • resetConsole—resets the switch console
Result	Displays a message after you click **Apply**.

Editing chassis information

About this task

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

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation pane, expand the **Configuration** > **Edit** folders.
3. Click **Chassis**.
4. Click the **Chassis** tab.
5. Edit the necessary options.
6. Click **Apply**.

Chassis field descriptions

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

Name	Description
Type	Specifies the chassis type.
ModelName	Specifies the chassis model name.
BrandName	Specifies the chassis brand name.
PartNumber	Specifies the device part number.
SerialNumber	Specifies a unique chassis serial number.
HardwareRevision	Specifies the current hardware revision of the device chassis.
NumSlots	Specifies the number of slots available in the chassis. • VSP 4000: 1 slot • VSP 7200 Series 2 slots • VSP 8200: 1 slot • VSP 8400: 4 slots
NumPorts	Specifies the number of ports currently installed in the chassis.

Table continues…

Name	Description
BaseMacAddr	Specifies the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
MacAddrCapacity	Specifies the number of routable MAC addresses based on the BaseMacAddr.
Temperature This parameter does not appear for all platforms.	Specifies the temperature of the device.
MacFlapLimitTime This parameter does not appear for all platforms.	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	Specifies the time interval, in seconds, after which auto-recovery runs on ports to clear actions taken by CP Limit or link flap. The default is 30.
MTUSize	Configures the maximum transmission unit size. The default is 1950.
MgidUsageVlanCurrent	Number of MGIDs for VLANs currently in use.
MgidUsageVlanRemaining	Number of remaining MGIDs for VLANs.
MgidUsageMulticastCurrent	Number of MGIDs for multicast currently in use.
MgidUsageMulticastRemaining	Number of remaining MGIDs for multicast.
DdmMonitor	Enables or disables the monitoring of the DDM. When enabled, the user gets the internal performance condition (temperature, voltage, bias, Tx power and Rx power) of the SFP/XFP. The default is disable.
DdmMonitorInterval	Configures the DDM monitor interval in the range of 5 to 60 in seconds. If any alarm occurs, the user gets the log message before the specific interval configured by the user. The default value is 5 seconds.
DdmTrapSend	Enables or disables the sending of trap messages. When enabled, the trap message is sent to the Device manager, any time the alarm occurs. The default is enable.
DdmAlarmPortdown	Sets the port down when an alarm occurs. When enabled, the port goes down when any alarm occurs. The default is disable.
PowerUsage This parameter does not appear for all platforms.	Specifies the amount of power the CPU uses.
PowerAvailable This parameter does not appear for all platforms.	Specifies the amount of power available to the CPU.

Viewing physical entities

Perform this procedure to view information about the functional components of the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Entity**.

Physical Entities field descriptions

Use the following table to use the Physical Entities tab.

Name	Description
Index	Indicates the index of the entry.
Descr	Indicates the name of the manufacturer for the physical entity.
VendorType	Indicates the vendor-specific hardware type for the physical entity. Because there is no vendor-specifier registration for this device, the value is 0.
ContainedIn	Indicates the index value for the physical entity which contains this physical entity. A value of zero indicates that this physical entity is not contained in any other physical entity.
Class	Indicates the general hardware type of the physical entity. The value is configured to the standard enumeration value that indicates the general class of the physical entity.
ParentRelPos	Indicates the relative position of the child component among the sibling components.
Name	Indicates the name of the component, as assigned by the local device, and that is suitable to use in commands you enter on the console of the device. Depending on the physical component naming syntax of the device, the name can be a text name such as console, or a component number such as port or module number. If there is no local name, there is no value.
HardwareRev	Indicates the vendor-specific hardware revision string for the physical entity. If no specific hardware revision string is associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value.

Table continues…

Name	Description
	If there is no information available, there is no value.
FirmwareRev	Indicates the vendor-specific firmware revision string for the physical entity.
	If no specific firmware programs are associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value.
	If there is no information available, there is no value.
SoftwareRev	Indicates the vendor-specific software revision string for the physical entity.
	If no specific software programs are associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value.
	If there is no information available, there is no value.
SerialNum	Indicates the vendor-specific serial number string for the physical entity. The value is the serial number string printed on the component, if present.
	If there is no information available, there is no value.
MfgName	Indicates the name of the manufacturer of the physical component. The value is the manufacturer name string printed on the component, if present.
	If the manufacturer name string associated with the physical component is unknown, then this object contains a zero-length string.
	If there is no information available, there is no value.
ModelName	Indicates the vendor-specific model name identifier string associated with the physical component. The value is the part number which is printed on the component.
	If the model name string associated with the physical component is unknown, then this object contains a zero-length string.
Alias	Indicates an alias name for the physical entity that is specified by a network manager, and provides a nonvolatile handle for the physical entity.
	The software supports read-only and provides values for the port interface only.
AssetID	Indicates a user-assigned asset tracking identifier for the physical entity. This value is specified by a

Table continues…

Name	Description
	network manager, and provides nonvolatile storage of this information.
	Because this object is not supported, there is no value.
IsFRU	Indicates whether or not the physical entity is considered a field replaceable unit.
	• If the value is `true(1)`, then the component is a field replaceable unit.
	• If the value is `false(2),` then the component is permanently contained within a field replaceable unit.
MfgDate	Indicates the manufacturing date of the managed entity. If the manufacturing date is unknown, then the value is `'0000000000000000'H`.
Uris	Indicates additional identification information about the physical entity.
	Uris is not supported, therefore there is no value.

Configuring system flags

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

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.
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.
AuthSuccessTrapEnable	Enable the trap send for login authentication success
MrouteStrLimit	Enable or disable Mroute stream limit in system. Disabled by default.
DataPathFaultShutdownEnable	Enable or disable data path fault shutdown. Enabled by default.
ForceTopologyIpFlagEnable	Activates or disables the flag that configures the CLIP ID as the topology IP. Values are true or false. The default is disabled.
CircuitlessIpId	Uses the CLIP ID as the topology IP. Enter a value from 1–256.

Configuring channelization

Use this procedure to enable or disable channelization on a port. Channelization configures the port to operate as four channels, or ports.

> ⓘ **Important:**
>
> Not all hardware platforms support the same port speeds or the channelization feature. For more information about feature support, see *Release Notes*.

About this task

> ✱ **Note:**
>
> Enabling or disabling channelization resets the port QoS configuration to default values. For information about configuring QoS values, see *Configuring QoS and ACL-Based Traffic Filtering*.

Procedure

1. In the Device Physical View tab, select a port that supports channelization.
2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.
3. Click **General**.
4. Click the **Channelization** tab.
5. To enable channelization on the port, select **enable** .
6. Click **Apply** . Alternatively, you can rignt-click the port on the Device Physical View tab, and then select **Channelization Enable**.

7. To disable channelization on a port, select the first sub-port for the corresponding port, slot/port/1.

8. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

9. Click **General**.

10. Click the **Channelization** tab.

11. To disable channelization on the port, select **disable** . This action will disable the four sub-ports.

12. Click **Apply** . Alternatively, you can rignt-click the port on the Device Physical View tab, and then select **Channelization Disable**.

Channelization field descriptions

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

Name	Description
Channelization	This field determines whether channelization is enabled or disabled on the selected port. The two options are **enable** and **disable**. The default is **disable**.

Configuring basic port parameters

About this task

Configure options for a basic port configuration.

When you use 1 Gigabit Ethernet SFP transceivers on VSP 7254XSQ, the software disables auto-negotiation on the port:

- If you use 1 Gbps fiber SFP transceivers, the remote end must also have auto-negotiation disabled.

- If you use 1 Gbps copper SFP transceivers, the remote end must have auto-negotiation enabled. If not, the link will not be established.

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Click **General**.

4. Click the **Interface** tab.

5. Configure the fields as required.

   10/100BASE-TX ports do not consistently auto-negotiate 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 auto-negotiation 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[/sub-port] format.
Name	Configures the name of the port.
Descr	Displays the description of the port. A textual string containing information about the interface.
Type	Displays the type of connector plugged in the port.
Mtu	Displays the Maximum Transmission Unit (MTU) for the port. The size of the largest datagram which can be sent or received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
PhysAddress	Displays the physical address of the port. The address of the interface at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
VendorDescr	Displays the vendor of the connector plugged in the port.
DisplayFormat	Identifies the slot and port numbers (slot/port). If the port is channelized, the format also includes the sub-port in the format slot/port/sub-port
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.
LicenseControlStatus	Shows the port license status. This field only applies to VSP 7200 Series.
ShutdownReason	Indicates the reason for a port state change.
LastChange	Displays the timestamp of the last change.
LinkTrap	Enable or disable link trapping.
AutoNegotiate	Enables or disables auto-negotiation for this port.

Table continues…

Name	Description
	The default is enabled for VSP 4000 Series and VSP 8000 Series but disabled for VSP 7200 Series.
AutoNegAd	Specifies the port speed and duplex abilities to be advertised during link negotiation.
	✱ **Note:**
	The 8424XT ESM does not support the following speeds: 10-full, 10-half, and 1000-half.
	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 the 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.
AdminDuplex	Configures the administrative duplex setting for the port.
	The switch does not support half duplex.
OperDuplex	Indicates the operational duplex setting for the port.
	The switch does not support half duplex.
AdminSpeed	Configures the administrative speed for the port.
OperSpeed	Indicates the operational speed for the port.
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).

Table continues…

Name	Description
MltId	Shows the MLT ID associated with this port. The default is 0.
Locked	Shows if the port is locked. The default is disabled.
UnknownMacDiscard	Discards packets that have an unknown source MAC address, and prevents other ports from sending packets with that same MAC address as the destination MAC address. The default is disabled.
DirectBroadcastEnable	Specifies if this interface forwards direct broadcast traffic.
OperRouting	Shows the routing status of the port.
HighSecureEnable	Enables or disables the high secure feature for this port.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
IpsecEnable	Enables or disables IP security (IPsec) on the interface. The default is disabled.
FlexUniEnable	Enables Flex UNI on the port. The default is disabled.
IngressRateLimit	Limits the traffic rate accepted by the specified ingress port.
IngressRatePeak	Configures the peak rate in Kbps. The default is 0. This parameter is not available on all platforms.
IngressRateSvc	Configures the service rate in Kbps. The default is 0. This parameter is not available on all platforms.
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 Kbps. The minimum egress rate limit that you can configure for the switch is 1000 Kbps. The maximum egress rate limit can vary by hardware. The **EgressRateLimit** field displays the maximum value. If the egress rate limit is configured to 0, it means this option is disabled.
TxFlowControl	Configures if the port sends pause frames. By default, an interface does not send pause frames. You must also enable the flow control feature globally before an interface can send pause frames.
TxFlowControlOperState	Shows the operational state of flow control.

Table continues…

Name	Description
BpduGuardTimerCount	Shows the time, starting at 0, since the port became disabled. When the BpduGuardTimerCount reaches the BpduGuardTimeout value, the port is enabled. Displays in 1/100 seconds.
BpduGuardTimeout	Specifies the value to use for port-state recovery. After a BPDU guard disables a port, the port remains in the disabled state until this timer expires. You can configure a value from 10 to 65535. The default is 120 seconds. If you configure the value to 0, the expiry is infinity.
BpduGuardAdminEnabled	Enables BPDU Guard on the port. The default 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 triggers a RIP update The default is none.
Result	Displays result of the selected action. The default is none.
IsPortShared	Indicates whether the port is combo or not. • portShared—Combo port. • portNotShared—Not a combo port. This parameter is not available on all platforms.
PortActiveComponent	Specifies whether the copper port is active or fabric port is active if port is a combo port. • fixed port—Copper port is active. • gbic port—Fabric port is active. This parameter is not available on all platforms.

Configuring IEEE 802.3X Pause frame transmit

Configure IEEE 802.3X Pause frame transmit to eliminate or minimize packet loss.

About this task

By default, flow control mode is disabled. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames.

By default, an interface does not send pause frames.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

2. Click **Chassis**.

3. Click the **Boot Config** tab.

4. For EnableFlowControlMode, select **enable**.

5. Click **Apply**.

6. Save the switch configuration.

7. Reboot the chassis, and log in again.

8. In the Device Physical View, select a port or ports.

9. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

10. Click **General**.

11. Click the **Interface** tab.

12. For TxFlowControl, select **enable** to enable the interface to generate pause frames.

13. Click **Apply**.

Viewing the boot configuration

About this task

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

Procedure

1. On the Device Physical View, select the Device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **Boot Config** tab.

Boot field descriptions

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

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time 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	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging earlier on specified port. It only works on console connection. By default, it is disabled. ❗ **Important:** Do not change this parameter.
EnableRebootOnError	Activates or disables automatic reboot on a fatal error. The default value is activated. ❗ **Important:** Do not change this parameter.
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled.
EnableRloginServer	Activates or disables the rlogin and rsh server. The default value is disabled.
EnableFtpServer	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the TFTPD flag is disabled.
EnableTftpServer	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
EnableSshServer	Activates or disables the SSH server service. The default value is disabled.
EnableSpbmConfigMode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. The boot flag is enabled by default.

Table continues…

Name	Description
EnableIpv6Mode	Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. This flag is disabled by default. This field does not appear for all hardware platforms.
EnableEnhancedsecureMode	Enables or disables the enhanced secure mode. Select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. The default is disabled. ✳ **Note:** It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
EnableUrpfMode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you configure it on a port or VLAN. The default is disabled.
EnableVxlanGwFullInterworkingMode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST. By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag. The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments. For more information about feature support, see *Configuring VLANs, Spanning Tree, and NLB*.
EnableFlowControlMode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames. The default is disabled.
EnableDvrLeafMode	Enables the switch to be configured as a DvR Leaf. When enabled, you cannot configure the switch to operate as a DvR Controller.
EnablevrfScaling	Changes the maximum number of VRFs and Layer 3 VSNs that the switch supports. If you select this

Table continues…

Name	Description
	check box, the maximum number increases. The default is disabled.
	❗ Important:
	If you select both this check box and the **EnableSpbmConfigMode** check box, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see *Release Notes*.

Configuring boot flags

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Chassis** folders.

2. Click the **Boot Config** tab.

3. Select the services you want to enable.

4. Click **Apply**.

Boot field descriptions

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

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time 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	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging

Table continues…

Name	Description
	earlier on specified port. It only works on console connection. By default, it is disabled. **❗ Important:** Do not change this parameter.
EnableRebootOnError	Activates or disables automatic reboot on a fatal error. The default value is activated. **❗ Important:** Do not change this parameter.
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled.
EnableRloginServer	Activates or disables the rlogin and rsh server. The default value is disabled.
EnableFtpServer	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the TFTPD flag is disabled.
EnableTftpServer	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
EnableSshServer	Activates or disables the SSH server service. The default value is disabled.
EnableSpbmConfigMode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. The boot flag is enabled by default.
EnableIpv6Mode	Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. This flag is disabled by default. This field does not appear for all hardware platforms.
EnableEnhancedsecureMode	Enables or disables the enhanced secure mode. Select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. The default is disabled. **✳ Note:** It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
EnableUrpfMode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you

Table continues…

Name	Description
	configure it on a port or VLAN. The default is disabled.
EnableVxlanGwFullInterworkingMode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST.
	By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag.
	The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments.
	For more information about feature support, see *Configuring VLANs, Spanning Tree, and NLB*.
EnableFlowControlMode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames.
	The default is disabled.
EnableDvrLeafMode	Enables the switch to be configured as a DvR Leaf.
	When enabled, you cannot configure the switch to operate as a DvR Controller.
EnablevrfScaling	Changes the maximum number of VRFs and Layer 3 VSNs that the switch supports. If you select this check box, the maximum number increases. The default is disabled.
	🛈 **Important:**
	If you select both this check box and the **EnableSpbmConfigMode** check box, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see *Release Notes*.

Enabling Jumbo frames

About this task

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

Procedure

1. On the Device Physical View, select the Device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **Chassis** tab.

5. In **MTU size**, select either 1950, 9600 or 1522.

6. Click **Apply**.

Configuring the date and time

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

About this task

⊛ **Note:**

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

Procedure

1. On the Device Physical View, select the Device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **User Set Time** tab.

5. Type and select the correct details.

6. 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

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 pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Click **General**.

4. Click the **CP Limit** tab.

5. Select the **AutoRecoverPort** check box.

6. Click **Apply**.

CP Limit field descriptions

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

Name	Description
AutoRecoverPort	Activates or disables auto recovery of the port from action taken by CP Limit or link flap features. The default value is disabled.

Configuring an IP address for the management port

Configure an IP address for the management port so that you can remotely access the device using the out-of-band (OOB) management port. The management port runs on a dedicated VRF.

The configured IP subnet must be globally unique because the management protocols can go through in-band (Global Router) or out-of-band ports (Management VRF).

This procedure only applies to hardware with a dedicated, physical management interface.

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.

- Do not configure a default route in the Management VRF.

- If you want out-of-band management, define a specific static route in the Management Router VRF to the IP subnet where your management application resides.

- If you initiate an FTP session from a client device behind a firewall, you should set FTP to passive mode.

- The switch gives priority to out-of-band management when there is reachability from both in-band and out-of-band. To avoid a potential conflict, do not configure any overlapping between in-band and out-of-band networks.

About this task

Configure an IP address for the management port so that you can remotely access the device using the out-of-band (OOB) management port. The management port runs on a dedicated VRF. Redirect all commands that are run on the management port to its VRF.

The configured IP subnet has to be globally unique because the management protocols can go through in-band or out-of-band ports.

> **⊛ Note:**
>
> Do not configure a default route in the Management VRF and instead use a static route. Inbound FTP does not work when a default route is configured at the Management VRF.
>
> When you initiate FTP, you should also set FTP to passive mode.

Procedure

1. In the navigation pane, expand the **Configuration** > **VRF Context View** folders.
2. Click **Set VRF Context View**.
3. Select **MgmtRouter**, VRF 512.
4. Click **Launch VRF Context View**.

   A new EDM webpage 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.
6. In the navigation pane, expand the **Configuration** > **Edit** folders.
7. Click **Mgmt Port**.
8. Click the **IP Address** tab.
9. Click **Insert**.
10. Configure the IP address and mask.
11. Click **Insert**.
12. Collapse 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.

Table continues…

Name	Description
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. Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable VRF scaling and SPBM mode, the system also reserves VLAN IDs 3500 to 3999. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
BrouterPort	Specifies if the management port is a brouter port rather than a routeable VLAN. You cannot change this value 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 switch is a 10/100/1000 Mb/s Ethernet port that you can use for an out-of-band management connection to the switch.

✳ **Note:**

This procedure only applies to hardware with a dedicated physical management interface.

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 the CLI to configure static routes.

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

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	Enables or disables auto-negotiation for this port. The default is enabled for VSP 4000 Series and VSP 8000 Series but disabled for VSP 7200 Series.
AdminDuplex	Specifies the administrative duplex mode for the management port. The default is full.
OperDuplex	Specifies the operational duplex configuration for this port.
AdminSpeed	Specifies the administrative speed for this port. The default is 100 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.

This procedure only applies to hardware with a dedicated, physical management interface.

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

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
Interface	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 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.

The switch supports IPv6 addressing with Ping, Telnet, and SNMP.

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

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
Interface	Specifies an index value that uniquely identifies the interface.
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.

Automatically reactivating the port of the SLPP shutdown

About this task

Use the following procedure to automatically reactivate the port that is shut down by the SLPP.

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Click **General**.

4. Click the **CP Limit** tab.

5. Select **AutoRecoverPort** to activate auto recovery of the port from the action taken by SLPP shutdown features. The default value is disabled.

6. Click **Apply**.

Editing serial port parameters

About this task

Perform this procedure to specify serial port communication settings. The serial port on the device is the console port. Depending on the hardware platform, the console port displays as console or 10101.

Procedure

1. In the Device Physical View tab, select the console port on the device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Serial Port**.

4. Edit the port parameters as required.

5. Click **Apply**.

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 8.

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 pane, expand the **Configuration** > **Security** > **Control Path** folders.

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 pane, expand the **Configuration** > **Security** > **Control Path** folders.

2. Click **General**.

3. Click the **Port Lock** tab.

4. In the **LockedPorts** box, click the ellipsis **(...)** button.

5. Click the desired port or ports.

6. Click **Ok**.

7. In the Port Lock tab, click **Apply**.

Port Lock field descriptions

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

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

Viewing power information

About this task

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

Procedure

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

Power Info field descriptions

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

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

Viewing power status on VSP 8400

Perform this procedure to view the power status for the chassis and cards.

Procedure

1. For VSP 8400 only, in the navigation pane, expand the **Configuration** > **Edit** folders.
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	Displays an index value that identifies the component.
PowerStatus	Displays the power status.
SlotDescription	Displays the slot number.
CardDescription	Identifies the chassis or type of card.

Viewing fan information

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

About this task

For platforms that support both back-to-front and front-to-back airflow, the airflow direction must be the same for both the power supply fans and the chassis fan.

Procedure

1. On the Device Physical View, select the Device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **Fan Info** tab.

Fan Info field descriptions

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

Name	Description
Id	Specifies the fan ID.
Status	Specifies the operation status of the fan.
AmbientTemperature This parameter is not supported on all platforms.	Specifies the temperature of the fan.
Type	Specifies the running speed type of the fan.
FlowType This parameter is not supported on all platforms.	Specifies whether the air flow is front-to-back or back-to-front.

Viewing USB information

About this task

View USB information.

✱ **Note:**

> This information may not apply to your hardware model. For more information about your model features, see your hardware documentation.

Procedure

1. On the Device Physical View, select the Device.

2. In the navigation pane, open the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **USB** tab.

Viewing topology status information

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** folders.

2. Click **Topology**.

3. Click the **Topology** tab.

Topology field descriptions

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

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

Viewing the topology message status

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** folders.

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.
SubPort	Specifies the channel of a channelized 40 Gbps port that received the topology message.
IpAddr	Specifies the IP address of the sender of the topology message.
SegId (RemPort)	Specifies the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Specifies the MAC address of the sender of the topology message.
ChassisType	Specifies the chassis type of the device that sent the topology message.
BkplType	Specifies the backplane type of the device that sent the topology message.
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.

Configuring a forced message control pattern

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Chassis** folders.

2. Click the **Force Msg Patterns** tab.

3. Click **Insert**.

4. In the **PatternId** field, enter a pattern ID number.

5. In the **Pattern** field, enter a message control pattern.

6. Click **Insert**.

Force Msg Patterns field descriptions

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

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

Chapter 9: Power over Ethernet fundamentals

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

To know which ports support PoE, see your hardware documentation.

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

> 😊 **Note:**
>
> This feature is not supported on all hardware platforms. For more information about the features supported on your hardware, see Release Notes.

You can configure PoE from CLI and Enterprise Device Manager (EDM).

PoE overview

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

> 🛈 **Important:**
>
> This feature is not supported on all hardware platforms. For more information about feature support, see *Release Notes*.

For more information about PoE and power supplies, see your hardware documentation.

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

The switch automatically detects each IEEE 802.3af-draft-compliant powered device attached to each front-panel port and immediately sends power to that appliance. The switch also automatically detects how much power each device requires and supply the required DC voltage at a set current

based on the load conditions and current availability. The switch supports both PoE and standard LAN devices.

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

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

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

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

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

PoE detection types

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

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

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

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

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

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

Power usage threshold

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

Port power limit

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

Port power priority

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

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

The priority methods are:

1. Port configured PoE priority

   - Low: (default) standard priority for standard devices

   - High: higher priority than low for important devices

   - Critical: highest priority for critical devices like wireless APs

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

PD Classification

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

Table 7: Classification chart for 802.3at

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

Table 8: Classification chart for 802.3af

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

PoE/PoE+ Allocation Using LLDP

✱ **Note:**

> This feature is not supported on all hardware platforms. For more information about feature support, see *Release Notes*

Power over Ethernet/Power over Ethernet Plus allocation using Link Layer Discovery Protocol (LLDP) supports Ethernet switches, which do not support hardware-level power negotiation. With this feature, these switches support IEEE-based PoE and play the role of power sourcing equipment (PSE).

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

⚠ **Important:**

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

✴ **Note:**

Some switches feature a hardware design that supports hardware-level detection. Therefore, they do not require LLDP.

For more information about support, see *Release Notes*.

Power over Ethernet configuration using CLI

Power over Ethernet (POE) is supported on the switch. This section provides details to configure PoE settings using CLI.

Disabling PoE on a port

About this task

Disable PoE on a port.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-
   port]][,...]}
   ``` or ```interface vlan <1-4059>
   ```

   ✴ **Note:**

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

2. Disable PoE on the port:

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

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

Next steps

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

Configuring PoE detection type

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

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

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

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

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal

2. Configure PoE detection type:

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

Variable definitions

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

Variable	Value
{802dot3af | 802dot3af_and_legacy | 802dot3at | 802dot3at_and_legacy}	Configures the detection type to one of the following values: • 802dot3af: Set PD detection mode in 802.3af • 802dot3af_and_legacy: Set PD detection mode in 802.3af and legacy • 802dot3at: Set PD detection mode in 802.3at • 802dot3at_and_legacy: Set PD detection mode in 802.3at and legacy

Configuring PoE power usage threshold

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the power usage threshold:

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

Variable definitions

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

Variable	Value
<1–99>	Specifies the PoE usage threshold in the range of 1—99 percent.

Configuring power limits for channels

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```
   or `interface vlan` *<1–4059>*

   ⭐ **Note:**

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

2. Configure PoE channel limits:

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

Variable definitions

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

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

Configuring port power priority

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-
   port]][,...]} or interface vlan <1-4059>
   ```

   > **Note:**
   >
   > If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure port power priority:

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

Variable definitions

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

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

Displaying PoE main configuration

About this task

Use this procedure to display the main PoE configuration.

Procedure

1. Enter Privileged EXEC mode:

   enable

2. View the main configuration:

   show poe-main-status

Example

```
Switch:1#show poe-main-status
================================================================================
                          PoE Main Status - Stand-alone
================================================================================
Available DTE Power        : 1855 Watts
DTE Power Status           : NORMAL
DTE Power Consumption      : 92 Watts
DTE Power Usage Threshold  : 80
PD Detect Type             : 802.3at and Legacy
Power Source Present       : AC Only
Primary Power Status       : Present and operational
Redundant Power Status     : Present and Operational
```

Displaying PoE port status

About this task

Use this procedure to display the PoE port status.

Procedure

1. Enter Privileged EXEC mode:

   enable

2. View the port status:

   show poe-port-status

Example

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

```
1/12      Enable  Searching           Class0       32       Low
1/13      Enable  Searching           Class0       32       Low
1/14      Enable  Searching           Class0       32       Low
1/15      Enable  Searching           Class0       32       Low
1/16      Enable  Searching           Class0       32       Low
1/17      Enable  Searching           Class0       32       Low
```

⊛ **Note:**

The PoE status of all ports is displayed. The preceding output is a sample of the full output.

Displaying port power measurement

About this task

Use this procedure to display the PoE power measurement.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View measurement information:

   `show poe-power-measurement`

Example

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

⊛ **Note:**

The PoE port measurement for all ports is displayed. The preceding output is a sample of the full output.

Power over Ethernet configuration using EDM

This section provides details to configure PoE settings using EDM.

Configuring PoE globally

About this task

Modify global PoE configuration.

Procedure

1. In the Device Physical View, select one or more ports that support PoE. For information about which ports support PoE, see your hardware documentation.

2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Click **General**.

4. Click the **PoE** tab.

5. Select the **AdminEnable** checkbox.

6. Select a value from the list—true to enable PoE for the port, or false to disable PoE for the port.

7. Select one of the following values to for **PowerPriority**:

   • critical

   • high

   • low

8. Enter the value of the power in the **PowerLimit(watts)** field.

9. To configure PoE for other selected ports, repeat steps 6 on page 152 through 8 on page 152.

10. Click **Apply**.

PoE field descriptions

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

Name	Description
Port	Shows the switch port number.
AdminEnable	Shows whether PoE is enabled or disabled on this port.
DetectionStatus	Shows the operational status of the powerdevice detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power

Table continues…

Name	Description
	• fault—power-specific fault detected on port • test—detecting device in test mode • otherFault
PoweClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Shows the power priority for the specified: • critical • high • low
PoweerLimit(Watts)	Shows the maximum power that the switch can supply to a port. The maximum power and system default power is 32W per port.
Voltage(volts)	Shows the power measured in volts.
Current(amps)	Shows the power measured in amps.
Power(Watts)	Shows the power measured in watts.

Viewing PoE information for specific switch ports

About this task

View the PoE configuration for specific switch ports

Procedure

1. In the Device Physical View, select one or more ports. For information about which ports support PoE, see your hardware documentation.

2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Click **General**.

4. Click the **PoE** tab.

PoE field descriptions

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

Name	Description
Port	Shows the switch port number.
AdminEnable	Shows whether PoE is enabled or disabled on this port.

Table continues…

Name	Description
DetectionStatus	Shows the operational status of the powerdevice detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault
PoweClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Shows the power priority for the specified: • critical • high • low
PoweerLimit(Watts)	Shows the maximum power that the switch can supply to a port. The maximum power and system default power is 32W per port.
Voltage(volts)	Shows the power measured in volts.
Current(amps)	Shows the power measured in amps.
Power(Watts)	Shows the power measured in watts.

Chapter 10: 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 ports.

Procedure

1. In the navigation pane, expand the **Configuration** > **Device** folders.

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 ports. 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

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

About this task

This procedure applies only to VSP 8400. VSP 8400 provides slots for four Ethernet Switch Modules (ESM).

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

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.

Viewing power supply parameters

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

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

2. Click **Power Supply**.

Detail field descriptions

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

Name	Description
Type	Describes the type of power used.
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	Display the input line voltage: • low 110v—power supply connected to a 110 Volt source • high 220v—power supply connected to a 220 Volt source • ac110vOr220v—power supply connected to a 110 Volt or 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.
OutputWatts	Displays the output power of this power supply.

Viewing temperature on the chassis

You can view information about the temperature on the chassis.

About this task

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

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

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **Temperature** tab.

Temperature field descriptions

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

Name	Description
CpuTemperature	Current CPU temperature in Celsius.
MacTemperature	Current MAC component temperature in Celsius.
Phy1Temperature	Current PHY 1 component temperature in Celsius. This field does not appear on all hardware platforms.
Phy2Temperature	Current PHY 2 component temperature in Celsius. This field does not appear on all hardware platforms.

Chapter 11: Domain Name Service

The following sections provide information on the Domain Name Service (DNS) implementation for the switch.

DNS fundamentals

This section provides conceptual material on the Domain Name Service (DNS) implementation for the switch. Review this content before you make changes to the configurable DNS options.

DNS client

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

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

- It is easier to remember a name than a full IP address.

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

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

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

DNS modifies Ping, Telnet, and copy applications. You can enter a hostname or an IP address to invoke Ping, Telnet, and copy applications.

A log/debug report is generated for all the DNS requests sent to DNS servers and all successful DNS responses received from the DNS servers.

IPv6 Support

The Domain Name Service (DNS) used by the switch supports both IPv4 and IPv6 addresses with no difference in functionality or configuration.

DNS configuration using CLI

This section describes how to configure the Domain Name Service (DNS) client using Command Line Interface (CLI).

DNS supports IPv4 and IPv6 addresses.

Configuring the DNS client

About this task

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

functionality or configuration using CLI.

You can configure connection for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the DNS client:

   ```
   ip domain-name WORD<0-255>
   ```

3. **(Optional)** Add addresses for additional DNS servers:

   ```
   ip name-server <primary|secondary|tertiary> WORD<0-46>
   ```

4. View the DNS client system status:

   ```
   show ip dns
   ```

Example

```
Switch:1> enable
```

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

Add addresses for additional DNS servers:

```
Switch:1(config)# ip name-server tertiary 254.104.201.141
```

Variable definitions

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

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.

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

About this task

Query the DNS host for information about host addresses.

You can enter either a hostname, 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 using CLI.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the host information:

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

Example

```
Switch:1> enable
```

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

View the host information:

```
Switch:1(config)# show hosts 10.10.10.1
```

Variable definitions

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

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).

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. Under the **DNS Servers** tab, in the **DnsServerListAddressType** box, you must select **ipv4** or **ipv6**.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** folders.
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 addresses with no difference in functionality or configuration in this procedure.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** folders.
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	Enter hostname or host IPv4 or IPv6 address to be identified.
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 12: Licensing

The following sections provide information on the Licensing features, activation, and installation on the switch.

Licensing fundamentals

This section provides conceptual information about feature licensing for the switch. Review this section before you make changes to the license configuration.

Feature licensing

> 🛈 **Important:**
>
> Prior to VOSS 4.1, VSP 4000 used the Avaya Data Licensing Portal to generate license files. This system produced a license file with the `.dat` extension. In VOSS 4.1 and later, VSP 4000 uses the Product Licensing and Delivery System (PLDS) as the license order, delivery, and management tool. PLDS produces a license file with the `.xml` extension. If you have older `.dat` license files on your switch, the software continues to support them. For more information, see

This product uses the Product Licensing and Delivery System (PLDS) as the license order, delivery and management tool. PLDS provides self-service license activations, upgrades, moves or changes.

> ✴ **Note:**
>
> PLDS supports only a single host (system MAC address) for each license file. You cannot use the same license file on multiple hosts.

PLDS Port License for VSP 7200 Series hardware

The VSP 7200 Series hardware models are now available with twenty four 1/10 GbE SFP/SFP+ and four 40 GbE QSFP+ ports enabled by default. To enable the remaining ports on the switch, you must purchase a Port License. The PLDS Port License can be used alone or can be combined with a PLDS Premier or Premier plus MACsec License at any time.

PLDS Premier License

The switch requires a Premier License for Layer 3 VSNs (including Multicast), Fabric Extend, MACsec, Distributed Virtual Routing (DvR), VXLAN Gateway, and 25 VRFs or higher features. These are in addition to the features covered by the Base License.

Because MACsec is not allowed in some countries, the following PLDS Premier licenses are offered with and without MACsec:

- **PLDS Premier License** – This license is required to enable and use the following features:

  - Fabric Connect Layer 3 Virtual Services Networks (VSNs)
  - Fabric Extend including the use of logical IS-IS interfaces
  - DvR
  - VXLAN Gateway
  - Greater than 24 VRFs and Layer 3 VSNs

- **PLDS Premier License plus MACsec** – This license is required to enable and use the following features:

  - Fabric Connect Layer 3 Virtual Services Networks (VSNs)
  - Fabric Extend including the use of logical IS-IS interfaces
  - IEEE 802.1AE MACsec
  - DvR
  - VXLAN Gateway
  - Greater than 24 VRFs and Layer 3 VSNs

- **PLDS Premier License to PLDS Premier License plus MACsec Uplift** – This license is for customers that want to upgrade their Premier License to a Premier License plus MACsec.

PLDS Premier License and Port License:

If you want to purchase PLDS Premier Licenses with a Port License, or upgrade your existing Premier Licenses to include a Port License, you have the following options:

- **PLDS Premier License plus Port License** – In addition to enabling the features supported by the Premier License, it enables the licensed ports on a VSP 7200 Series switch.

- **PLDS Premier License plus MACsec plus Port License** – In addition to enabling the features supported by the Premier license and the MACsec feature, it enables the licensed ports on a VSP 7200 Series switch.

Premier Trial License:

For customers that would like to trial premier features prior to purchasing a Premier License, there are the following two types of PLDS Premier Trial Licenses that permit the use of premier features for a 60 day period. During the trial period you can configure all features without restriction, including system console and log messages.

- **PLDS Premier Trial License** – This license is for Layer 3 VSNs including Multicast and Fabric Extend, but you cannot configure MACsec.

- **PLDS Premier Trial License plus MACsec** – This license is for MACsec and Layer 3 VSNs including Multicast and Fabric Extend.

✳ **Note:**

Port Licenses are not available with the trial versions of the PLDS Premier Licenses.

The PLDS Premier Trial License is generated using the system MAC address of a switch and can only be generated and used *once* for a given MAC address.

System console and log messages alert you to the expiry of the 60 day trial period. The message `Licence trial period will expire in ## days` appears every 24 hours. At the end of the trial period, the following message appears: `License trial period has expired. All the Premier features will be disabled. Please buy the license to enable them.` This message is the last notification recorded.

The system logs the preceding messages even if you do not use or test license features during the trial period. If you load a valid license on the system, it does not record the preceding messages.

After the expiry of the 60 day trial period, you will also see messages in the alarms database that the license has expired. If you restart the system after the license expiration, the Premier features will not be loaded even if they are in the saved configuration.

If you purchase a Premier License, you must obtain and install a license file. For more information about how to generate a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300; All licensing activities are performed through the Avaya PLDS Portal at http://plds.avaya.com.

Base License

The Base License is included with the switch hardware and activates the features not included in the Premier License.

The Base License includes the following Layer 2 features:

- VLANs
- RSTP
- MSTP
- MLT
- IGMP
- 802.1AX Link Aggregation (LACP)
- 802.1ag
- SPB Core/Base (NNI)
- Layer 2 Virtual Service Networks (VSNs)
- Etree
- Layer 2 Virtual Service Networks (VSN) with Multicast
- Virtualized Multicast over Fabric Connect*
- Fabric Attach
- Switched UNI

The Base License includes the following Layer 3/Routing features:

- Global Routing Table (GRT) IP Routing including IP-Shortcuts
- Terminal Access Controller Access Control System Plus (TACACS+)
- Service Level Agreement Monitor (SLA Mon™)
- Inter-ISID-Routing
- VRRP

- DHCP-Relay
- RIP in the GRT and VRF
- RIP in the GRT with IP Shortcuts
- OSPF in the GRT and VRF
- OSPF in the GRT with IP Shortcuts
- BGP in the GRT and VRF
- BGP in the GRT with IP Shortcuts
- SPB in the GRT with IP Shortcuts
- Multicast using IP-Shortcuts
- GRT with IP Shortcuts
- Route Policy Virtualization in the GRT and the GRT with IP Shortcuts
- IP Multicast Routing parity with IGMP v1, v2, and v3
- IP VRF
- IPv6
- IPv6 Alternative Routes
- IPv4 and IPv6 Multicast Route Statistics
- Per-queue rate limiting
- SMLT
- Switched UNI

License type and part numbers

The following table provides the part number for the various licenses supported on the switch.

Table 9: Supported licenses

Part number/ Order code	License type
380176	Premier license for one chassis
380177	Premier license with MACsec for one chassis
380178	Trial license
380179	Trial license with MACsec
380800	Premier to Premier license with MACsec

Feature license files

After you obtain the license file to enable the Premier License features, you must install the license file on the system to unlock the associated licensed features. You must load a license file on the internal flash of the device.

Transition to PLDS

The section provides information about the transition from the original three-tier licensing system to the new PLDS.

Original 3-tier system

Prior to Release 4.1, VSP 4000 employed a three-tier licensing system:

- the Base Software License
- the Advanced License
- the Premier License

The Base Software License was free of charge and more advanced features could be purchased separately, if required. The following table shows the three tiers and the features they supported.

Table 10: Data Licensing Portal three–tier system

Base (Layer 2 features)	Advanced (Layer 3 features)	Premier (Layer 3 Virtualization and MACsec)

• Core Layer 2 switching, ACLs, policers, shapers, 802.1D/w/s, 802.1p/Q
• MLT/LACP
• SPB base functionality
• SPB L2 VSNs
• SPB IEEE 802.1ag CFM
	• IP routing features:
	  - GRT IP routing
	  - SPB IP shortcuts
	  - SPB Inter-ISID routing
	  - VRRP
	  - DHCP relay
		• Layer 3 virtualization features:
		  - IP VRFs
		  - SPB L3 VSNs with Static Routing
		  - MACsec

License files in this three-tier system used the `.dat` extension.

PLDS 2-tier system

Beginning in Release 4.1, VSP 4000 uses PLDS as the license order, delivery and management tool. PLDS provides a two–tier framework: a Base Software License and a Premier License.

The Base Software License is free of charge with the purchase of VSP 4000 hardware. You can purchase a Premier License to unlock additional features. For more information about the two tiers and the features they support, see <u>Feature licensing</u> on page 164.

PLDS license files use the `.xml` extension.

Upgrading to 4.1 or later

When you upgrade your VSP 4000 deployment to VOSS 4.1 or later, previously purchased and installed licenses continue to operate. You do not need to convert old license files.

VOSS 4.1 and later ignore previously installed Advanced licenses because features enabled by Advanced licenses are now part of the Base Software License.

The procedure to install and load licenses on a switch remains the same. Note that the PLDS license file type is `.xml` as opposed to the `.dat` extension that was used by the older licensing system. If you have both a `.dat` license file and a `.xml` license file in the `/intflash/` directory, the `.xml` file receives preference.

You should leave the existing Advanced license installations intact on the switch so that there is no impact to licensed features in the unlikely event of a software downgrade to Release 4.0 or earlier.

For information about Avaya PLDS, see *Getting Started with Avaya PLDS for Avaya Networking Products, NN46199-300*.

For information and procedures about how to install licenses, see the following tasks:

- License installation using CLI on page 169
- License installation using EDM on page 172

License installation using CLI

Install and manage a license file for the switch by using the Command Line Interface (CLI).

Installing a license file

Before you begin

- File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
- You must enable the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server depending on which protocol you use to download the license file to the device.
- Ensure that you have the correct license file with the base MAC address of the switch on which you need to install the license. Otherwise, the system does not unblock the licensed features.

About this task

Install a license file on the switch to enable licensed features.

⊛ **Note:**

You can enable FTP or TFTP in the boot config flags and then initiate an FTP or a TFTP session from your workstation to put the file on the server running on the switch.

Procedure

1. From a remote station, or PC, use FTP or TFTP to download the license file to the device, and store the license file in the /intflash directory.

2. Enter Global Configuration mode:

   `enable`

   `configure terminal`

3. To load the license file, execute the following command:

   `load-license`

   ### ❗ Important:

   If the loading fails, or if the switch restarts and cannot locate a license file in the specified location, the switch cannot unlock the licensed features and reverts to base functionality.

   ### ❗ Important:

   The license filename stored on a device must meet the following requirements:

   - Maximum of 63 alphanumeric characters

   - No spaces or special characters allowed

   - Underscore (_) is allowed

   - The file extension ".xml" is required

   If more than one valid .xml license file exists in the /intflash/ directory, the switch uses the license with the highest capability.

Example

 Use FTP to transfer a license file from a PC to the internal flash on the device:

```
C:\Users\jsmith>ftp 192.0.2.16
Connected to 192.0.2.16 (192.0.2.16).
220 FTP server ready
Name (192.0.2.16:(none)): rwa
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put premier_macsec.xml  /intflash/premier_macsec.xml
local: premier_macsec.xml remote: /intflash/premier_macsec.xml
227 Entering Passive Mode (192,0,2,16,4,2)
150 Opening BINARY mode data connection
226 Transfer complete
101 bytes sent in 2.7e-05 secs (3740.74 Kbytes/sec)
ftp>
```

Log in to the device and load the license. The following example shows a successful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1 [06/12/15 15:59:57.636:UTC] 0x000005bc 00000000 GlobalRouter SW INFO
License Successfully Loaded From </intflash/premier_macsec.xml> License Type -- PREMIER
+MACSEC
```

The following example shows an unsuccessful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1  [06/12/15 15:58:48.376:UTC] 0x000006b9 00000000 GlobalRouter SW
INFO Invalid license file /intflash/license_Switch_example.xml  HostId is not Valid

CP1  [06/12/15 15:58:48.379:UTC] 0x000005c4 00000000 GlobalRouter SW INFO No Valid
License found.
```

Variable definitions

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

Variable	Value
<a.b.c.d>	Specifies the IPv4 and IPv6 address of the TFTP server from which to copy the license file.
<file>	Specifies the name of the license file when copied to the flash. The destination file name must meet the following requirements: • Maximum of 63 alphanumeric characters • No spaces or special characters allowed • Underscore (_) is allowed • The file extension ".xml" is required
<srcfile>	Specifies the name of the license file on the TFTP server. For example, license.xml.

Showing a license file

About this task

Display the existing software licenses on your device.

Procedure

1. Log on to the switch to enter User EXEC mode.

2. Show the existing software licenses on your device:

   ```
   show license
   ```

Example

For no license:

```
Switch:1>show license
No license file is loaded.
Premier feature set is available without license for development environment

**********************************************************************
Features requiring a Premier license:
        -  Layer 3 VSNs
        -  MACsec
        -  Fabric Extend
        -  DVR
```

The output for the "show license" cli command for legacy licenses will show non-zero values for MD5 of Key and MD5 of file:

```
Switch:1>show license


        License file name     :     /intflash/premier.dat
        License Type          :     PREMIER
        MD5 of Key            :     7ce34d20 0caf0074 6657d928 1b4a0a18
        MD5 of File           :     9e0e5a4c 4855efb1 90909c11 bb870d84
        Generation Time       :     2015/08/12 01:53:39
        Expiration Time       :
        Base Mac Addr         :     b4:47:5e:37:9a:00
        flags                 :     0x00000001 SINGLE
        memo                  :



**********************************************************************
Features requiring a Premier license:
        -  Layer 3 VSNs
        -  MACsec
        -  Fabric Extend
        -  DVR
```

The output for the "show license" cli command for PLDS licenses will show all zeroes for MD5 of Key and MD5 of file:

```
Switch:1>show license

        License file name     :     /intflash/premier_macsec.xml
l
        License Type          :     PREMIER+MACSEC
        MD5 of Key            :     00000000 00000000 00000000 00000000
        MD5 of File           :     00000000 00000000 00000000 00000000
        Generation Time       :     2015/2/26 11:09:53
        Expiration Time       :
        Base Mac Addr         :     b0:ad:aa:46:f0:00
        flags                 :     0x00000001 SINGLE
        memo                  :



**********************************************************************
Features requiring a Premier license:
        -  Layer 3 VSNs
        -  MACsec
        -  Fabric Extend
        -  DVR
```

License installation using EDM

Install and manage a license file for the switch 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 switch on which you need to install the license. Otherwise, the system does not unblock the licensed features.

About this task

Install a license file on the switch to enable licensed features.

IPv4 and IPv6 addresses are supported.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.

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 have a file extension of .xml.

6. Select **start**.

7. Click **Apply**.

   The license file is copied to the flash of the device. The status of the file copy appears in the Result field.

8. In the navigation pane, expand the **Configuration** > **Edit** folders.

9. Click **Chassis**.

10. Click the **System** tab.

11. In **ActionGroup1**, select **loadLicense**.

12. Click **Apply**.

    > 🛈 **Important:**
    >
    > If the loading fails, the switch cannot unlock the licensed features and reverts to base functionality.

13. On the **System** tab, in **ActionGroup1**, select **saveRuntimeConfig**.

14. Click **Apply**.

> ❗ **Important:**
>
> The license filename stored on a device must meet the following requirements:
>
> - Maximum of 63 alphanumeric characters
> - No spaces or special characters allowed
> - Underscore (_) is allowed
> - The file extension ".xml" is required

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

Viewing license file information

About this task

View information about the license file for the switch.

Procedure

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

2. Click **Chassis**.

3. Click the **License** tab.

License field descriptions

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

Name	Description
FileName	Indicates the file name of the current license. ★ **Note:** If this field is empty it indicates that there is no license installed on the switch.
LicenseType	Indicates the level type of the current license.
DurationType	Indicates the duration type of the current license.
FactoryTrialPeriodRemainingDays	Indicates the days left before the factory default trial period expires. ★ **Note:** This applies only to the license type **trialFactoryDefault**. For other license types, the field displays **0**.
GenerationTime	Indicates the date on which the license file was generated. ★ **Note:** If there is no license installed on the system, this field displays **0000000000000000 H**.
ExpirationTime	Indicates the date on which the license file expired. ★ **Note:** If there is no license installed on the system, this field displays **0000000000000000 H**.

Chapter 13: Link Layer Discovery Protocol

The following sections describe how to use Link Layer Discovery Protocol (LLDP).

Link Layer Discovery Protocol (802.1AB) fundamentals

With Link Layer Discovery Protocol (LLDP) you can obtain node and topology information to help detect and correct network and configuration errors.

LLDP

802.1AB is the IEEE standard called Station and Media Access Control Connectivity Discovery. This standard defines the Link Layer Discovery Protocol.

LLDP stations connected to a local area network (LAN) can advertise station capabilities to each other, allowing the discovery of physical topology information for network management.

LLDP-compatible stations can comprise any interconnection device, including PCs, IP Phones, switches, and routers.

Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

The functions of an LLDP station include:

- Advertising connectivity and management information about the local station to adjacent stations

- Receiving network management information from adjacent stations

- Enabling the discovery of certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers

  For example, you can use LLDP to discover duplex mismatches between an IP Phone and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

The following figure shows an example of a LAN using LLDP.
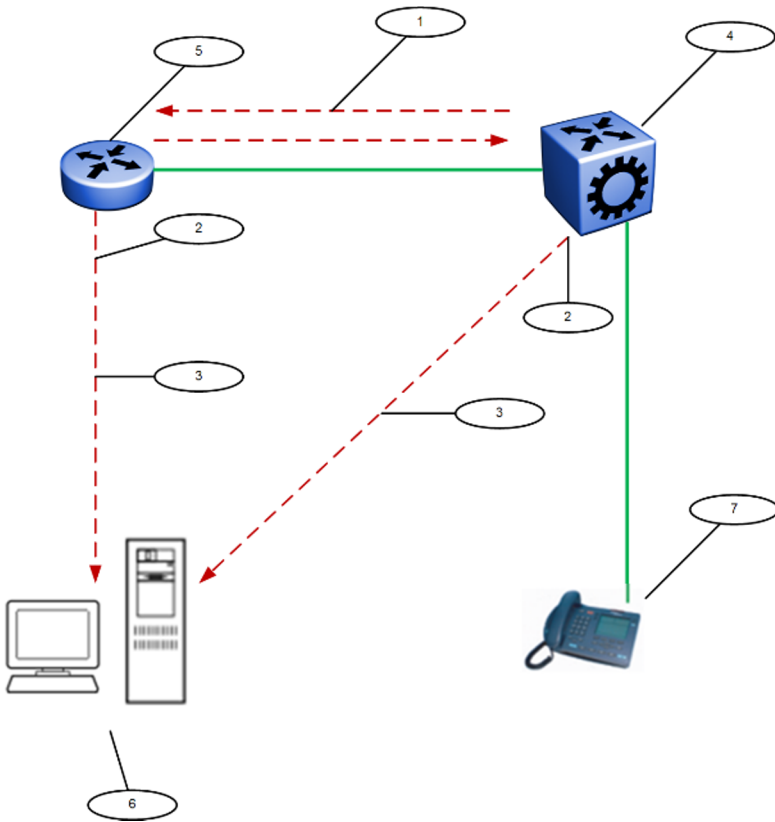
Figure 2: LLDP in a LAN

Legend:

1. The switch and an LLDP-enabled router advertise chassis and port IDs and system descriptions to each other

2. The devices store the information about each other in local MIB databases, accessible with SNMP

3. A network management system retrieves the data stored by each device and builds a network topology map

4. Switch

5. Router

6. Management work station

7. IP Phone

LLDP modes

LLDP is a one-way protocol.

An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier.

The LLDP agent also can receive information about the capabilities and current status of the system associated with a remote MSAP identifier.

However, LLDP agents cannot solicit information from each other.

Modes:

You can configure the local LLDP agent to

- Transmit and receive

Connectivity and management information

The information parameters in each LLDP frame are in a Link Layer Discovery Protocol Data Unit (LLDP PDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDP PDU includes the following mandatory TLVs:

- Chassis ID
- Port ID
- Time To Live
- Port Description
- System Name
- System Description
- System Capabilities (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDP PDU information from the MSAP identifier remains valid.

The receiving LLDP agent automatically discards all LLDP PDU information, if the sender fails to update it in a timely manner.

A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDP PDU MSAP identifier.

Transmitting LLDP PDUs

When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDP PDU.

LLDP PDUs are regularly transmitted at a user-configurable transmit interval (tx-interval) or when any of the variables in the LLPDU is modified on the local system; for example, system name or management address.

Transmission delay (tx-delay) is the minimum delay between successive LLDP frame transmissions.

TLV system MIBs

The LLDP local system MIB stores the information to construct the various TLVs for transmission.

The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDP PDU and TLV error handling

The system discards LLDP PDUs and TLVs that contain detectable errors.

The system assumes that TLVs that contain no basic format errors, but that it does not recognize, are valid and stores them for retrieval by network management.

LLDP and MultiLink Trunking

You must apply TLVs on a per-port basis.

Because LLDP manages trunked ports individually, TLVs configured on one port in a trunk do not propagate automatically to other ports in the trunk.

And the system sends advertisements to each port in a trunk, not on a per-trunk basis.

LLDP and Fabric Attach

Fabric Attach uses LLDP to signal a desire to join the SPB network. When a switch is enabled as an FA Server, it receives IEEE 802.1AB LLDP messages from FA Client and FA Proxy devices requesting the creation of Switched UNI service identifiers (I-SIDs). All of the discovery handshakes and I-SID mapping requests are using LLDP TLV fields. Based on the LLDP standard, FA information is transmitted using organizational TLVs within LLDP PDUs.

FA also leverages LLDP to discover directly connected FA peers and to exchange information associated with FA between those peers.

Link Layer Discovery Protocol configuration using CLI

This section describes how to configure Link Layer Discovery Protocol using the Command Line Interface (CLI).

IPv4 management IP addresses are supported by LLDP, including the management virtual IP address, and they are advertised in the Management address TLV.

Configuring global LLDP transmission parameters

Before you begin

- In the GigabitEthernet Interface Configuration mode, specify the LLDP port status as transmit only or transmit and receive.

About this task

Use this procedure to configure global LLDP transmission parameters on the switch. If required, you can also restore these parameters to their default values.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal
   ```

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

⊛ **Note:**

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

2. To configure the LLDP transmission parameters, enter:

```
lldp [tx-interval|tx-hold-multiplier]
```

3. **(Optional)** To restore specific LLDP transmission parameters to their default values, enter:

```
default lldp [tx-interval|tx-hold-multiplier]
```

4. **(Optional)** To restore all LLDP transmission parameters to their default values, enter:

```
default lldp
```

Example

Configure the LLDP transmission interval. The LLDP port status is set to transmit and receive prior to the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#lldp status txAndRx
Switch:1(config-if)#exit
Switch:1(config)#lldp tx-interval 31
```

Optionally, restore the LLDP transmission interval to its default value:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#default lldp tx-interval
```

Variable definitions

Use the information in the following table to help you understand the `lldp` command.

Variable	Value
tx-interval<*5–32768*>	Specifies the global LLDP transmit interval in seconds, that is, the interval in which LLDP frames are transmitted. The default is 30 seconds.
tx-hold-multiplier <*2–10*>	Configures the multiplier for the transmit interval used to compute the Time To Live (TTL) value in LLDP frames. The default is 4 seconds.

Configuring LLDP status on ports

About this task

Use this procedure to configure LLDP and configure the status to transmit and receive on a port, or ports, on your switch.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ✱ **Note:**

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

2. To configure LLDP and configure the status for transmit and receive on a port or ports, enter:

   ```
   lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   status <txAndRx>
   ```

3. To configure LLDP to the default setting for a port or ports, enter:

   ```
   default lldp port {slot/port[/sub-port] [-slot/port[/sub-port]]
   [,...]} status <txAndRx>
   ```

Example

Configure LLDP on your switch and set the status for transmit and receive on a port:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#lldp status txAndRx
```

Restore LLDP port status to the default value. The default status is *disabled*.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#default lldp status
```

Disable LLDP on your switch:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#no lldp status
```

Variable definitions

Use the data in the following table to use the **lldp port** command.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
status *<txAndRx>*	Configures the LLDP Data Unit (LLDP PDU) transmit and receive status on the port(s). • default—restores LLDP port parameters to default values • txAndrx—enables LLDP PDU transmit and receive

Enabling CDP mode on a port

In order to use CDP compatible mode, you must enable it on a port, or ports, on your switch.

If CDP is enabled, the interface accepts only CDP packets. Similarly, if CDP is disabled but LLDP is enabled, the interface accepts only LLDP packets.

To switch a port from CDP mode to LLDP mode, the LLDP status on that port must be txAndrx.

About this task

Do not enable CDP mode if you plan to use the port with an ONA or Fabric Attach.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   > ⭐ **Note:**
   >
   > If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. To enable CDP, enter the following command:

   ```
   lldp cdp enable
   ```

3. To disable CDP, enter the following command:

   ```
   no lldp cdp enable
   ```

Example

To enable CDP on a port:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#lldp cdp enable
```

⭐ **Note:**

To switch a port from CDP mode to LLDP mode, LLDP status on that port must be txAndrx.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#no lldp cdp enable
```

To shutdown LLDP or CDP on a port:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1>(config-if)#no lldp status
```

Variable definitions

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

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
cdp <enable>	Configures the CDP-compatible mode on the port(s). • no—disables the CDP-compatible mode • default—restores the CDP-compatible mode to the default value The default is disabled.

Viewing global LLDP information

About this task

Use this procedure to view global LLDP information, to know which LLDP settings and parameters are configured.

Procedure

1. Enter Privileged EXEC mode:

   enable

2. To verify global LLDP information, enter:

```
show lldp {local-sys-data|[neighbor port {slot/port[/sub-port] [-
slot/port[/sub-port]] [,...]}]|[port {slot/port[/sub-port] [-slot/
port[/sub-port]] [,...]}] |[rx-stats port {slot/port[/sub-port] [-
slot/port[/sub-port]] [,...]}]|[stats]|[tx-stats port {slot/port[/
sub-port] [-slot/port[/sub-port]] [,...]}]}
```

Example

View global LLDP information:

```
Switch:1#show lldp
802.1ab Configuration:
----------------------------------
            TxInterval: 30
      TxHoldMultiplier: 4
           ReinitDelay: 1
               TxDelay: 1
  NotificationInterval: 5
```

View the LLDP local system data on the switch:

```
Switch:1#show lldp local-sys-data

======================================================================
                         LLDP Local System Data

======================================================================

            ChassisId: MAC Address        b0:ad:aa:4c:54:00
            SysName  : LLDP agent
            SysDescr : <model-name> (<release-number>)  BoxType: <model-name>
            SysCap   : Br / Br
----------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,      R= Repeater,
S= Station,   T= Telephone, W= WLAN,       r= Router
```

View the LLDP neighbor information. You can also view this on a specific port.

```
Switch:1#show lldp neighbor

==========================================================================
                            LLDP Neighbor
==========================================================================

Port: 1/28       Index    : 1                    Time: 0 day(s), 01:16:25
                 Protocol : LLDP
                 ChassisId: MAC Address      a4:25:1b:52:54:00
                 PortId   : MAC Address      a4:25:1b:52:54:1b
                 SysName  : BEB
                 SysCap   : Br / Br
                 PortDescr: <model-name> - Gbic1000BaseT Port 1/28
                 SysDescr : <model-name> (<release-number>)
                 Address  : 10.13.13.47
--------------------------------------------------------------------------

Total Neighbors : 1


--------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,      R= Repeater,
S= Station,   T= Telephone, W= WLAN,       r= Router
```

View the LLDP administrative status of all ports on the switch. You can also view this on a specific port.

```
Switch:1#show lldp port

====================================================================
                        LLDP Admin Port Status

====================================================================
--------------------------------------------------------------------
Port        AdminStatus  ConfigNotificationEnable  CdpAdminState
--------------------------------------------------------------------
1/1         txAndRx      disabled                  disabled
1/2         txAndRx      disabled                  disabled
1/3         txAndRx      disabled                  disabled
1/4         txAndRx      disabled                  disabled
...
...
```

View the LLDP reception statistics. You can also view this on a specific port.

```
Switch:1#show lldp rx-stats

==============================================================================
                            LLDP Rx-Stats

==============================================================================

Port        Frames      Frames   Frames   TLVs        TLVs         AgeOuts
Num         Discarded   Errors   Total    Discarded   Unsupported
                                          (Non FA)    (Non FA)
------------------------------------------------------------------------------
1/1         0           0        0        0           0            0
1/2         0           0        0        0           0            0
1/3         0           0        0        0           0            0
1/4         0           0        0        0           0            0
...
...
```

View the LLDP statistics:

```
Switch:1#show lldp stats

==========================================================
                        LLDP Stats

==========================================================
Inserts     Deletes    Drops     Ageouts
----------------------------------------------------------
4           0          0         0
----------------------------------------------------------
```

View the LLDP transmission statistics:

```
Switch:1#show lldp tx-stats

====================================================================
                        LLDP Tx-Stats

====================================================================

PORT NUM                    FRAMES
--------------------------------------------------------------------
1/1                         95
1/2                         95
```

```
1/3                      95
1/4                      95
1/5                      95
...
...
```

Variable definitions

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

Variable	Value
local-sys-data	Displays the LLDP local system data.
neighbor [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP neighbor system information. You can also view this on a specific port.
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
port [*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP administrative status of a port or all ports on the switch.
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
rx-stats [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP reception statistics on all ports on the switch, or on a specific port.
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
stats	Displays the LLDP statistics.
tx-stats [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP transmission statistics on all ports on the switch or on a specific port.
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is

Table continues…

Variable	Value
	channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing LLDP neighbor information

Display information about LLDP neighbors to help you configure LLDP for maximum benefit.

About this task

Use this procedure to display LLDP neighbor information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To view LLDP neighbor information, enter:

   ```
   show lldp neighbor [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

Example

```
Switch:1#show lldp neighbor

================================================================================
                              LLDP Neighbor
================================================================================

Port: 2/1        Index    : 1                    Time: 0 day(s), 00:19:59
                 Protocol   : LLDP
                 ChassisId: MAC Address        a4:25:1b:50:64:00
                 PortId   : MAC Address        a4:25:1b:50:64:34
                 SysName  : Switch1
                 SysCap   : Br / Br
                 PortDescr: 2/1
                 Address  : 10.19.12.98
                 SysDescr : <model-name> (<release-number>)  BoxType: <model-name>
--------------------------------------------------------------------------------
Total Neighbors : 1
--------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,   O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

Variable definitions

Use the data in the following table to use the **show lldp neighbor** command.

Variable	Value
port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Displays LLDP neighbor information on the specified port.
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of

Variable	Value
	slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing global LLDP statistics

Use this procedure to view and verify global LLDP statistics.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To view LLDP statistics, enter:

   ```
   show lldp stats
   ```

3. To view LLDP reception statistics, enter:

   ```
   show lldp rx-stats
   ```

4. To view LLDP transmission statistics, enter:

   ```
   show lldp tx-stats
   ```

5. **(Optional)** Clear global LLDP statistics:

   ```
   clear lldp stats summary
   ```

Example

View LLDP statistics:

```
Switch:1>enable
Switch:1#show lldp stats

================================================================
                              LLDP Stats
================================================================
Inserts    Deletes    Drops      Ageouts
----------------------------------------------------------------
0          0          0          0
----------------------------------------------------------------
```

View LLDP transmission statistics:

```
Switch:1#show lldp tx-stats
================================================================
                              LLDP Tx-Stats
================================================================

PORT NUM                FRAMES
----------------------------------------------------------------
1/2                     100
```

View LLDP reception statistics:

```
Switch:1#show lldp rx-stats


===============================================================
                            LLDP Rx-Stats
===============================================================

Port   Frames       Frames    Frames   TLVs        TLVs          AgeOuts
Num    Discarded    Errors    Total    Discarded   Unrecognized
---------------------------------------------------------------
1/2    0            0         46       0           0             0
```

Viewing port-based LLDP statistics

Use this procedure to verify port-based LLDP statistics.

About this task

LLDP operates at the interface level. Enabling FA on a port automatically enables LLDP transmission and reception on the port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in the MLT.

⊛ **Note:**

When FA is enabled on ports in an MLT or LACP MLT, tagging is enabled and spanning tree is disabled on those ports.

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

Procedure

1. Enter Privileged EXEC mode:

    ```
    enable
    ```

2. To verify successful LLDP transmission on a port, enter:

    ```
    show lldp tx-stats port {slot/port[/sub-port] [-slot/port[/sub-
    port]] [,...]}
    ```

3. To verify that a port receives LLDP PDUs successfully, enter:

    ```
    show lldp rx-stats port {slot/port[/sub-port] [-slot/port[/sub-
    port]] [,...]}
    ```

4. **(Optional)** To clear LLDP statistics on a port, or ports, enter:

    ```
    clear lldp stats {slot/port[/sub-port] [-slot/port[/sub-port]]
    [,...]}
    ```

Example

Verify LLDP transmission statistics on a port:

```
Switch:1>en
Switch:1#show lldp tx-stats port 1/2
================================================================
                               LLDP Tx-Stats
================================================================

PORT NUM                 FRAMES
----------------------------------------------------------------
1/2                      100
```

Verify that the port is receiving LLDP PDUs:

```
Switch:1#show lldp rx-stats port 1/2

===============================================================================
                               LLDP Rx-Stats
===============================================================================

Port       Frames      Frames    Frames    TLVs        TLVs          AgeOuts
Num        Discarded   Errors    Total     Discarded   Unsupported
                                           (Non FA)    (Non FA)
-------------------------------------------------------------------------------
1/2        0           0         46        0           0             0
```

Link Layer Discovery Protocol configuration using EDM

This section describes how to configure LLDP on your switch using EDM.

Configuring LLDP global information

Use this procedure to configure or view LLDP global information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **Globals** tab.

3. After you make the required configuration changes, click **Apply** to save changes.

Globals field descriptions

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

Field	Description
lldpMessageTxInterval	Specifies the interval at which LLDP messages are transmitted.

Table continues…

Field	Description
	The default is 30 seconds.
lldpMessageTxHoldMultiplier	Specifies the multiplier used to calculate the time-to-live (TTL) value of an LLDP message.
	The default value is 4 seconds.
lldpReinitDelay	Specifies the delay in seconds between the time a port is disabled and the time it is re-initialized.
	The default is 1 second.
lldpTxDelay	Specifies the delay in seconds between successive LLDP transmissions.
	The default is 1 second.
	The recommended value is as follows:
	1 < **lldpTxDelay** < (0.25 x **lldpMessageTxInterval**)
lldpNotificationInterval	Specifies the time interval between successive LLDP notifications. It controls the transmission of notifications.
	The default is 5 seconds.
Stats	
RemTablesLastChangeTime	Specifies the timestamp of LLDP missed notification events on a port, for example, due to transmission loss.
RemTablesInserts	Specifies the number of times the information advertised by a MAC Service Access Point (MSAP) is inserted into the respective tables.
RemTablesDeletes	Specifies the number of times the information advertised by an MSAP is deleted from the respective tables.
RemTablesDrops	Specifies the number of times the information advertised by an MSAP was not entered into the respective tables.
RemTablesAgeouts	Specifies the number of times the information advertised by an MSAP was deleted from the respective tables.

Viewing the LLDP port information

Use this procedure to view the LLDP port information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **Port** tab.

3. View the administrative status of the port in the **AdminStatus** field. To modify, double-click on a cell and select a value from the drop-down list.

4. View whether the port is enabled for notifications in the **NotificationEnable** field. To modify, double-click on a cell and select a value from the drop-down list.

5. View the set of TLVs whose transmission using LLDP is always allowed by network management in the **TLVsTxEnable** field.

6. **(Optional)** Modify the TLVs as follows:

   a. To enable a TLV, select the appropriate check box, and click **Ok**. You can select more than one check box.

   b. To enable all TLVs, click **Select All**, and click **Ok**.

   c. To disable all TLVs, click **Disable All**, and click **Ok**.

7. View the CDP administrative status in the **CdpAdminState** field. To modify, double-click on a cell and select a value from the drop-down list.

8. Click **Apply** to save any configuration changes.

9. Click **Refresh** to verify the configuration.

Port field descriptions

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

Name	Description
PortNum	Specifies the port number. This is a read-only cell.
AdminStatus	Specifies the administrative status of the port. The options are: • txOnly: LLDP frames are only transmitted on this port. • rxOnly: LLDP frames are only received on this port. • txAndRx: LLDP frames are transmitted and received on this port. • disabled: LLDP frames are neither transmitted or received on this port. Any information received on this port from remote systems before this is disabled, ages out. The default is disabled.
NotificationEnable	Specifies whether the port is enabled or disabled for notifications. • true: indicates that the notifications are enabled. • false: indicates that the notifications are disabled. The default is false.
TLVsTxEnable	Specifies the set of TLVs whose transmission using LLDP is always allowed by network management. The following list describes the TLV types: • portDesc — indicates that the Port Description TLV is transmitted. • sysName — indicates that the System Name TLV. is transmitted. • sysDesc — indicates that the System Description TLV. is transmitted. • sysCap — indicates that the System Capabilities TLV. is transmitted.

Table continues…

Name	Description
	The default is an empty set of TLVs.
CdpAdminState	Specifies the CDP administrative status of the port.
	• true: indicates CDP is enabled.
	• false: indicates CDP is disabled.
	The default is false.
	If CDP is enabled, the interface accepts only CDP packets. Similarly, if CDP is disabled but LLDP is enabled, the interface accepts only LLDP packets. To switch a port from CDP mode to LLDP mode, the LLDP status on that port must be txAndRx.

Viewing LLDP transmission statistics

Use this procedure to view the LLDP transmission statistics. You can also view the statistics graphically.

About this task

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in that MLT.

⁕ **Note:**

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.

⁕ **Note:**

If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **TX Stats** tab.

   The transmission statistics are displayed.

3. To view the transmission statistics graphically for a port:

   a. In the content pane (on the right-hand-side), select a row and click the **Graph** button.

      The **TX Stats-Graph,<port-number>** tab displays.

      You can view a graphical representation of the LLDP frames transmitted (**FramesTotal**), for the following parameters:

- AbsoluteValue
- Cumulative
- Average/sec
- Minimum/sec
- Maximum/sec
- LastVal/sec

   b. To view the graph, select one of the above parameters and click the appropriate icon on the top left-hand-side of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

   c. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

   d. Click **Export**, to export the statistical data to a file.

   e. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

TX Stats field descriptions

Use the data in the following table to view the LLDP transmission statistics.

Field descriptions for the **TX Stats** tab.

Name	Description
PortNum	Specifies the port number.
FramesTotal	Specifies the total number of LLDP frames transmitted.

Field descriptions for the **TX Stats-Graph, <port-number>** tab.

Name	Description
AbsoluteValue	Specifies the absolute number of LLDP frames at a given point in time.
Cumulative	Specifies the cumulative rate of change of LLDP frames transmitted.
Average/sec	Specifies the average rate of change of LLDP frames transmitted.
Minimum/sec	Specifies the minimum rate of change of LLDP frames transmitted.
Maximum/sec	Specifies the maximum rate of change of LLDP frames transmitted.
LastVal/sec	Specifies the rate of change of LLDP frames transmitted in the last second.

Viewing LLDP reception statistics

Use this procedure to view the LLDP reception statistics. You can also view these statistics graphically.

About this task

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in that MLT.

★ **Note:**

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.

★ **Note:**

If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **RX Stats** tab.

3. To view the reception statistics graphically for a port:

   a. Select a row and click **Graph**.

      The **RX Stats-Graph,<port-number>** tab displays.

      You can view a graphical representation of the following data:

      • **FramesDiscardedTotal** — Total number of LLDP received frames that were discarded.

      • **FramesErrors** — Total number of erroneous LLDP frames received.

      • **FramesTotal** — Total number of frames received.

      • **TLVsDiscardedTotal** — Total number of received TLVs that were discarded.

      • **TLVsUnrecognizedTotal** — Total number of unrecognized TLVs received.

   b. Select one of the above parameters and click the appropriate icon on the top left-hand-side corner of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

c. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

d. Click **Export**, to export the statistical data to a file.

e. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

RX Stats field descriptions

Use the data in the following table to view the LLDP reception statistics.

Name	Description
PortNum	Specifies the port number.
FramesDiscardedTotal	Specifies the number of LLDP frames received on the port, but discarded, for any reason.
	This counter provides an indication of possible LLDP header formatting problems in the sending system, or LLDP PDU validation problems in the receiving system.
FramesErrors	Specifies the number of invalid LLDP frames received on the port.
FramesTotal	Specifies the total number of LLDP frames received on the port.
TLVsDiscardedTotal	Specifies the number of LLDP TLVs discarded on the port, for any reason.
TLVsUnrecognizedTotal	Specifies the number of LLDP TLVs on the port, that are unrecognized on that port.
	An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001–111 1110). An unrecognized TLV could be, for example, a basic management TLV from a later LLDP version.
AgeoutsTotal	Specifies the number of LLDP age-outs that occur on a specific port.
	An age-out is the number of times the complete set of information advertised by a particular MSAP is deleted, because the information timeliness interval has expired.

Field descriptions for the **RX Stats-Graph, <port-number>** tab.

Name	Description
AbsoluteValue	Specifies the absolute number of LLDP frames at a given point in time.
Cumulative	Specifies the cumulative rate of change of LLDP frames received.
Average/sec	Specifies the average rate of change of LLDP frames received.
Minimum/sec	Specifies the minimum rate of change of LLDP frames received.
Maximum/sec	Specifies the maximum rate of change of LLDP frames received.
LastVal/sec	Specifies the rate of change of LLDP frames received in the last second.

Viewing LLDP local system information

Use this procedure to view the LLDP local system information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **Local System** tab.

Local System field descriptions

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

Name	Description
ChassisIdSubType	Indicates the encoding used to identify the local system chassis. • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Indicates the chassis ID of the local system.
SysName	Indicates local system name.
SysDesc	Indicates local system description.
SysCapSupported	Indicates the system capabilities supported on the local system.
SysCapEnabled	Indicates the system capabilities that are enabled on the local system.

Viewing LLDP local port information

Use this procedure to view the LLDP local port information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **Local Port** tab.

Local port field descriptions

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

Name	Description
PortNum	Indicates the port number.

Table continues…

Name	Description
PortIdSubType	Indicates the type of port identifier. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Indicates the identifier associated with the port, on the local system.
PortDesc	Indicates the description of the port, on the local system.

Viewing LLDP neighbor information

Use this procedure to view the LLDP neighbor information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.

2. In the content pane, click the **Neighbor** tab.

Neighbor field descriptions

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

Name	Description
TimeMark	Indicates the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Identifies the port on which the remote system information is received.
Index	Indicates a particular connection instance that is unique to the remote system.
ChassisIdSubtype	Indicates the type of encoding used to identify the remote system chassis. • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName

Table continues…

Name	Description
	• local
ChassisId	Indicates the chassis ID of the remote system.
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities enabled on the remote system.
SysName	Indicates the name of the remote system.
SysDesc	Indicates the description of the remote system.
PortIdSubType	Indicates the type of encoding used to identify the remote port.
PortId	Indicates the remote port ID.
PortDesc	Indicates the remote port description.
ProtocolType	Indicates whether the entry protocol is CDP or LLDP.
IpAddress	Indicates the neighbor's IP address.

Chapter 14: Network Time Protocol

The following sections provide information on the Network Time Protocol (NTP).

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 NTP client on the switch 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, the switch, 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 the switch 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.
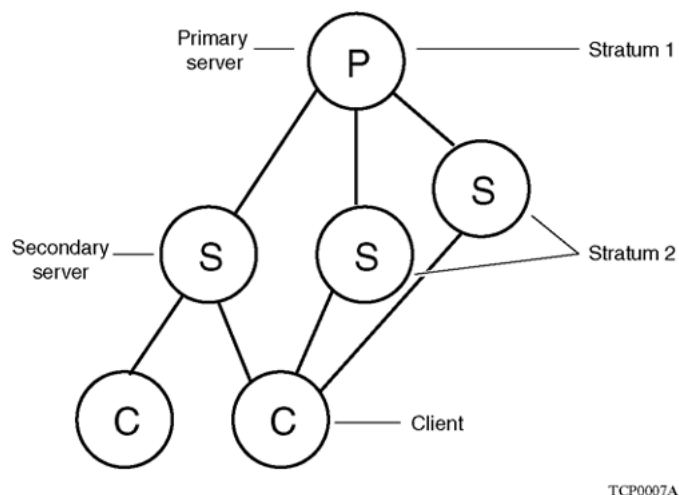
Figure 3: NTP time servers forming a synchronization subnet

In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary 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 201. 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.

Use the **show ntp statistics** command to verify the NTP synchronization status. For more information, see NTP server statistics on page 292. 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. The switch 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 203. 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.
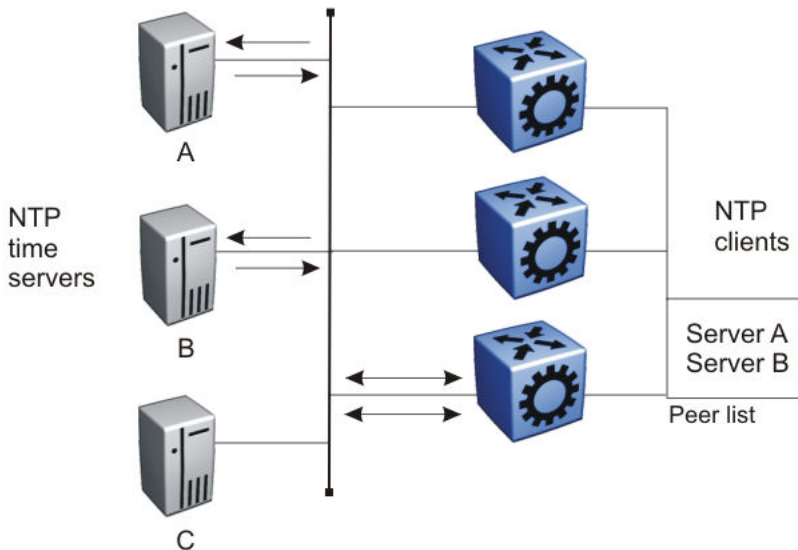
Figure 4: NTP time servers operating in unicast client mode

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, the switch uses the Message Digest 5 (MD5) or the Secure Hash Algorithm 1 (SHA1) algorithm to produce a message digest of the key. The message digest is created using the key and the message, but the key itself is not sent. Depending on which algorithm you select, the MD5 or SHA1 algorithm verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

To authenticate the message, the client authentication key must match that of the time server. Therefore, you must securely distribute the authentication key in advance (the client administrator must obtain the key from the server administrator and configure it on the client).

While a server can know many keys (identified by many key IDs), it is possible to declare only a subset of these as trusted. The time server uses this feature to share keys with a client that requires authenticated time and that trusts the server, but that is not trusted by the time server.

NTP configuration using CLI

This section describes how to configure the Network Time Protocol (NTP) using Command Line Interface (CLI).

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see *Configuring IPv4 Routing*.

 Important:

NTP server MD5 authentication or SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

This task flow shows the sequence of procedures you perform to configure NTP.
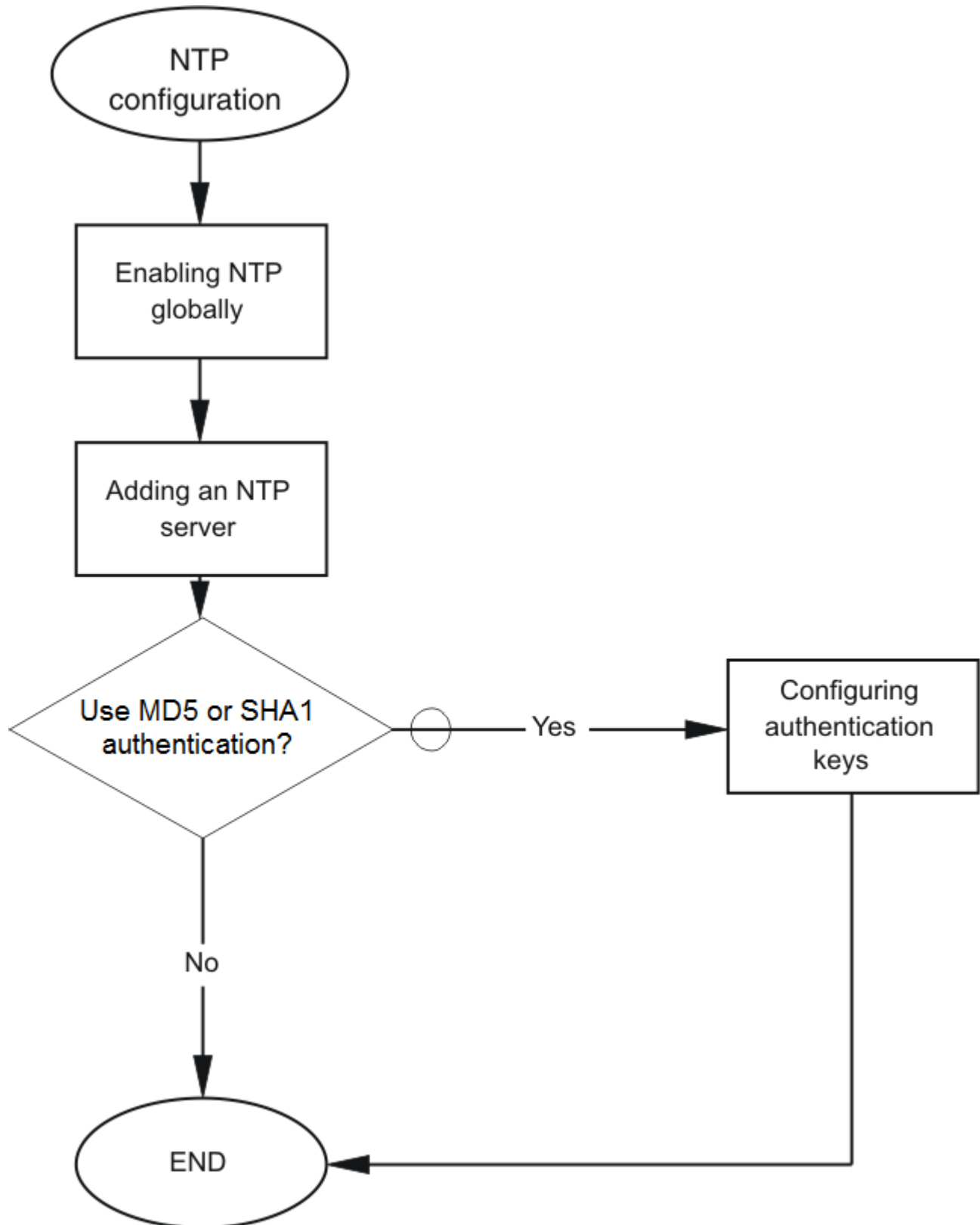
Figure 5: NTP configuration procedures

Enabling NTP globally

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. **(Optional)** Set the time interval between NTP updates or leave it at the default of 15 minutes:

   ```
   ntp interval <10-1440>
   ```

   > 🛈 **Important:**
   >
   > If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

3. Enable NTP globally:

   ```
   ntp
   ```

4. Create an authentication key:

   ```
   ntp authentication-key <1-2147483647> WORD<0-20> type <md5|sha1>
   ```

Example

Specify the interval between NTP updates to 10 minutes, and then enable NTP globally.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp interval 10
Switch:1(config)#ntp
```

Create an authentication key.

```
Switch:1(config)#ntp authentication-key 1 test type sha1
```

Variable definitions

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

Variable	Value
authentication-key <1-2147483647> WORD<0–20>	Creates an authentication key for MD5 or SHA1 authentication. To set this option to the default value, use the default operator with the command. The default configuration is to delete the authentication key.

Table continues…

Variable	Value
	NTP server MD5 or SHA1 authentication does not support passwords (keys) that start with a special character or contain a space between characters.
	WORD<0–20> specifies the secret key.
interval *<10-1440>*	Specifies the time interval, in minutes, between successive NTP updates.
	• The interval is expressed as an integer in a range from 10–1440. The default value is 15.
	If you changed the interval and then wanted to reset it back to the default, use the `default ntp interval` command.
type *<md5 | sha1>*	Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

Adding an NTP server

About this task

Add an NTP server or modify existing NTP server parameters by performing this procedure. You can configure a maximum of 10 time servers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Add an NTP server:

   ```
   ntp server <A.B.C.D>
   ```

3. Configure additional options for the NTP server:

   ```
   ntp server <A.B.C.D> [auth-enable] [authentication-key
   <0-2147483647>] [source-ip WORD <0-46>]
   ```

4. Activate the NTP server:

   ```
   ntp server <A.B.C.D> enable
   ```

Example

```
Switch:> enable
Switch:1 configure terminal
Switch:1(config)# ntp server 192.0.2.187
```

Variable definitions

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

Variable	Value
A.B.C.D	Specifies the IP address of the NTP server.
auth-enable	Activates MD5 or SHA1 authentication on this Network Time Protocol (NTP) server. Without this option, the NTP server will not have any authentication by default.
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 or SHA1 digest for the NTP server. The default authentication key is 0, which indicates disabled authentication.
source-ip WORD <0-46>	Specifies the source IP for the server. If you do not configure source-ip, by default, the source-ip entry is initialized to 0.0.0.0. The IP address specified can be any local interface.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.

Configuring authentication keys

About this task

Configure NTP authentication keys to use MD5 or SHA1 authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an authentication key:

   ```
   ntp authentication-key <1-2147483647> WORD<0-8> [type <md5|sha1>]
   ```

3. Enable MD5 or SHA1 authentication for the server:

   ```
   ntp server <A.B.C.D> auth-enable
   ```

4. Assign an authentication key to the server:

   ```
   ntp server <A.B.C.D> authentication-key <0-2147483647>
   ```

Example

```
Switch:1> enable
Switch:1# configure terminal
```

Create the authentication key:

```
Switch:1#(config)# ntp authentication-key 5 test type md5
```

Enable MD5 authentication for the NTP server:

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

Assign an authentication key to the server:

```
Switch:1#(config)# ntp server 192.0.2.187 authentication-key 5
```

Variable definitions

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

Variable	Value
A.B.C.D	Specifies the IP address of the server.
auth-enable	Activates MD5 or SHA1 authentication on this NTP server. The default is no authentication. To set this option to the default value, use the default operator with the command.
authentication-key <1-2147483647> WORD<0–20>	Creates an authentication key for MD5 or SHA1 authentication. To set this option to the default value, use the default operator with the command. The default configuration is to delete the authentication key.
authentication-key <0-2147483647>	Specifies the key ID value used to generate the MD5 or SHA1 digest for the NTP server. The value range is an integer from 0–2147483647. The default value is 0, which indicates disabled authentication. To set this option to the default value, use the default operator with the command.
type <md5|sha1>	Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

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 switch and ensure that the NTP server is reachable through this interface. For instructions, see *Configuring IPv4 Routing*.

ⓘ **Important:**

NTP server MD5 authentication or SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

This task flow shows you the sequence of procedures you perform to configure NTP.
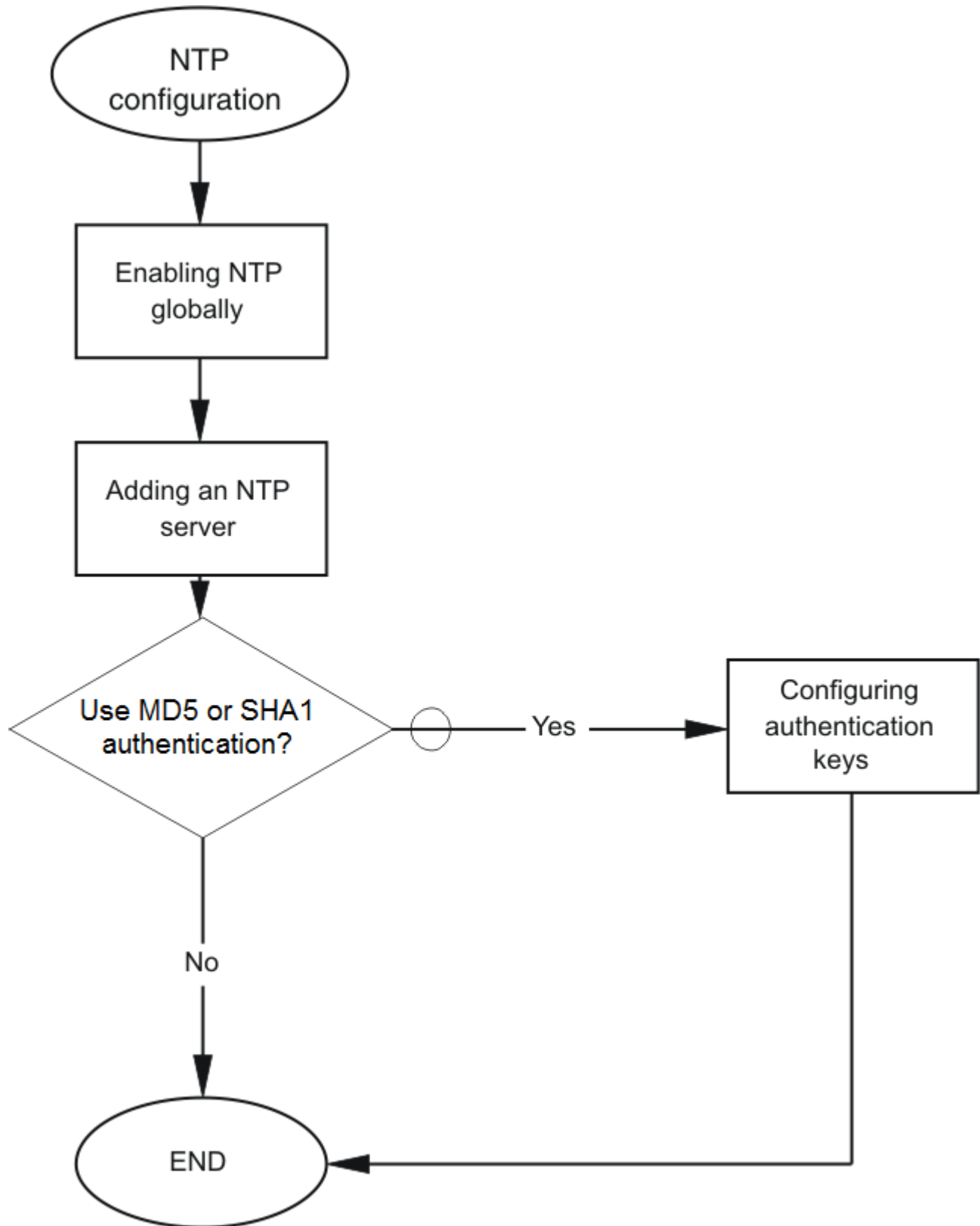
Figure 6: NTP configuration procedures

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 pane, expand the **Configuration** > **Edit** folders.

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 pane, expand the **Configuration** > **Edit** folders.

2. Click **NTP**.

3. Click the **Server** tab.

4. Click **Insert**.

5. Specify the IP address of the NTP server.

6. Click **Insert**.

   The IP address of the NTP server that you configured appears on the Server tab.

Server field descriptions

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

Name	Description
ServerAddress	Specifies the IP address of the remote NTP server.
Enable	Activates or disables the remote NTP server. The default is enabled.
Authentication	Activates or disables MD5 or SHA1 authentication on this NTP server. MD5 or SHA1 produces a message digest of the key. MD5 or SHA1 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The default is no authentication.
KeyId	Specifies the key ID used to generate the MD5 or SHA1 digest for this NTP server. You must specify a number between 1–214743647. The default is 0, which indicates that authentication is disabled.
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 pane, expand the **Configuration** > **Edit** folders.

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 or SHA1 digest. You must specify a value between 1–214743647. The default value is 1, which indicates that authentication is disabled.
KeySecret	This field is the MD5 or SHA1 key that generates the MD5 or SHA1 digest. You must specify an alphanumeric string between 0–20. 🛈 **Important:** You cannot specify the number sign (#) as a value in the KeySecret field. The NTP server interprets the # as the beginning of a comment and truncates all text entered after the #.
KeyType	This field specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

Chapter 15: Secure Shell

The following sections describe how to use Secure Shell (SSH) to enable secure communications support over a network for authentication, encryption, and network integrity.

Secure Shell fundamentals

Methods of remote access such as Telnet or FTP generate unencrypted traffic. Anyone that can see the network traffic can see all data, including passwords and user names. Secure Shell (SSH) is a client and server protocol that specifies the way to conduct secure communications over a network. Secure Shell can replace Telnet and other remote login utilities. Secure File Transfer Protocol (SFTP) can replace FTP with an encrypted alternative.

> * **Note:**
>
> If both SSH and SFTP are concurrently active, you have the ability to disable SFTP while allowing SSH to remain active. For more information, see Disabling SFTP without disabling SSH on page 235.

The switch software supports Secure CoPy protocol (SCP), which is a secure file transfer protocol. Use SCP to securely transfer files between a local host and a remote host. SCP is in off state by default, but you can turn it on when you enable SSH using the `boot config flags` command in the global config mode. The switch supports SCP only as an SCP server, which means that clients can send files to the switch or can request files from the switch. Secure CoPy (SCP) can replace FTP with an encrypted alternative.

Secure Shell supports a variety of the different public and private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key encrypts all traffic between the client and the server. The switch supports Secure Shell version 2 (SSHv2).
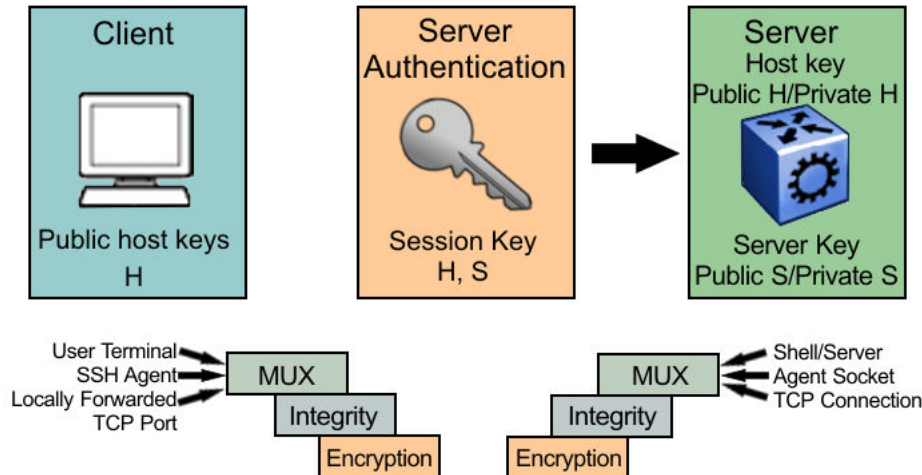
Figure 7: Overview of the SSHv2 protocol

By using a combination of host, server, and session keys, the SSHv2 protocol can provide strong authentication and secure communication over an insecure network, offering protection from the following security risks:

- IP spoofing
- IP source routing
- Domain name server (DNS) spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping and password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

The SSH secure channel of communication does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

With the SSHv2 server in the switch, you can use an SSHv2 client to make a secure connection to the switch and work with commercially available SSHv2 clients. For more information about supported clients, see Table 12: Tested software on page 222. The switch also supports outbound connections to remote SSHv2 servers to provide complete inbound and outbound secure access.

Security features

The SSHv2 protocol supports the following security features:

- Authentication. This feature determines, in a reliable way, the SSHv2 client. During the log on process, the SSHv2 client is queried for a digital proof of identity.

  Supported authentications with the switch as a server for SSHv2, are: RSA, DSA, and passwords. Supported authentications with the switch as a client for SSHv2, are: DSA and passwords. The switch does not support RSA when the switch acts as a client.

  When the switch acts as an SSH server, by default the switch allows a maximum of only four sessions, although it can accommodate up to eight sessions at a time. However, only one SSH public key encryption per access level is allowed at a time. For instance, if multiple SSH public key encryption clients need to connect to the server with the same access level, such as rwa,

then the clients must connect to the server one-by-one as the switch only supports one public key per access level.

- Encryption. The SSHv2 server uses encryption algorithms to scramble data and render it unintelligible except to the receiver.

  Supported encryption and ciphers are: 3DES, AES128-cbc, AES192-cbc, AES256-cbc, AES128–ctr, AES192-ctr, AES256-ctr, MD5, secure hash algorithm 1 (SHA-1) and SHA-2.

- Integrity. This feature guarantees that the data transmits from the sender to the receiver without alterations. If a third party captures and modifies the traffic, the SSHv2 server detects this alteration.

SSHv2 considerations using EDM

You must use CLI to initially configure SSHv2. You can use Enterprise Device Manager (EDM) to change the SSHv2 configuration parameters. CLI is the recommended user interface for SSHv2 configuration and it is recommended that you use the console port to configure the SSHv2 parameters. Depending on the hardware platform, the console port displays as console or 10101.

❗ Important:

Do not enable SSHv2 secure mode using Configuration and Orchestration Manager (COM). If you enable SSHv2 secure mode, then the system disables Simple Network Management Protocol (SNMP). This locks you out of a COM session. Enable SSH secure mode using CLI or EDM.

SSHv2 secure mode is different from enhanced secure mode and hsecure. SSHv2 secure mode disables unsecure management protocols on the device such as FTP, rlogin, SNMP, Telnet, and TFTP. SSHv2 secure mode is enabled through the `ssh secure` command.

When you enable SSHv2 secure mode, the system disables FTP, rlogin, SNMPv1, SNMPv2, SNMPv3, Telnet and TFTP. After SSHv2 secure mode is enabled, you can choose to enable individual non-secure protocols. However, after you save the configuration and restart the system, the non-secure protocol is again disabled, even though it is shown as enabled in the configuration file. After you enable SSHv2 secure mode, you cannot enable non-secure protocols by disabling SSHv2 secure mode.

You can disable block-snmp after you enable SSHv2 secure mode, and you can connect again using COM.

SSHv2 support for IPv6

On IPv6 networks, the switch supports SSHv2 server only. The switch does not support outbound SSHv2 client over IPv6. On IPv4 networks, the switch supports both SSHv2 server and SSHv2 client.

Interoperability

The SSHv2 client can operate with the following SSHv2 servers:

- Another VOSS switch
- ERS 8600/8800
- Linux running Open SSH
- VSP 7000
- VSP 9000

Outbound connections

The SSHv2 client supports SSHv2 DSA public key authentication and password authentication.

😎 **Note:**

You must enable SSH globally before you can generate SSH DSA user keys.

The SSHv2 client is a secure replacement for outbound Telnet. Password authentication is the easiest way to use the SSHv2 client feature.

Instead of password authentication, you can use DSA public key authentication between the SSHv2 client and an SSHv2 server. Before you can perform a public key authentication, you must generate the key pair files and distribute the key files to all the SSHv2 server systems. Because passphrase encrypts and further protects the key files, you must provide a passphrase to decrypt the key files as part of the DSA authentication.

To attempt public key authentication, the SSHv2 client looks for the associated DSA key pair files in the /intflash/.ssh directory. If no DSA key pair files are found, the SSHv2 client automatically prompts you for password authentication. If the SSHv2 client succeeds with the authentication, then a new secured SSHv2 session is established to the remote SSHv2 server. For more information, see Table 13: DSA authentication access levels and file names on page 223.

⚠️ **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 SSHv2 connection, then the system defaults back to the password authentication. If the SSHv2 client succeeds with the authentication, then a new secured SSHv2 session is established to the remote SSHv2 server.

SSH version 2

SSH version 2 (SSHv2) protocol is a complete rewrite of the SSHv1 protocol. In SSHv2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH Transport Layer manages the server authentication and provides the initial connection between the client and the server. After the connection is established, the Transport Layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

  The SSH Authentication Protocol runs on top of the SSH Transport Layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  The SSH Connection Protocol runs on top of the SSH Transport Layer and user authentication protocols. SSH-CONN provides interactive logon sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

The following figure shows the three layers of the SSHv2 protocol.

Administering VOSS
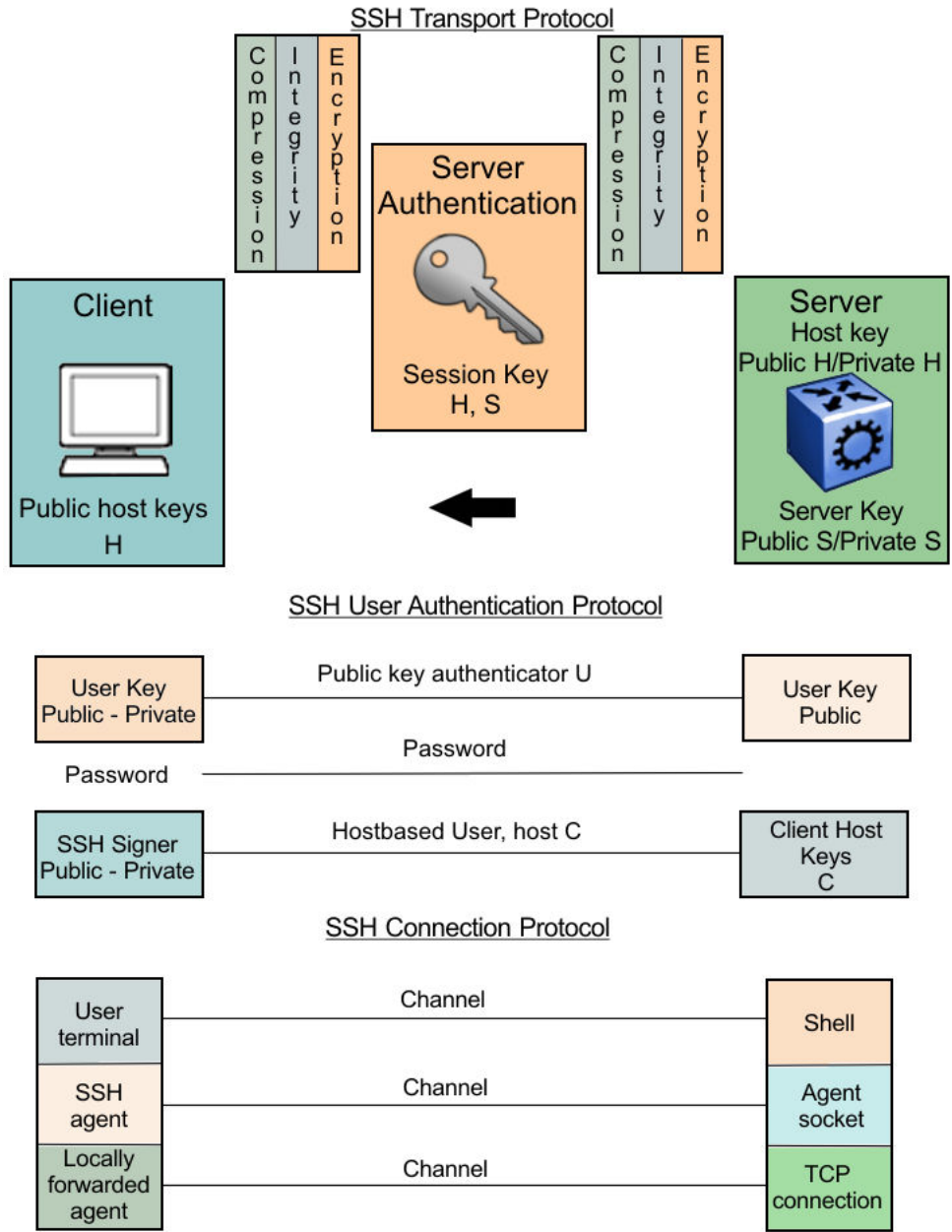
Figure 8: Separate SSH version 2 protocols

The modular approach of SSHv2 improves on the security, performance, and portability of the SSHv1 protocol.

⊘ Important:

The SSHv1 and SSHv2 protocols are not compatible. The switch does not support SSHv1.

User ID log of an SSH session established by SCP client

The switch logs the user ID of an SSH session initiated by the SCP client. If an SCP client establishes an SSH session, the message appears in the following format:

```
CP1 [08/06/15 09:43:42.230:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH user
authentication succeeded for user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:42.232:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH SCP session
start by  user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:44.020:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SCP session
closed by  user rwa on host 10.68.231.194
CP1 [08/06/15 09:43:44.021:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH session
closed by user rwa on host 10.68.231.194
```

In the preceding example log output, rwa is the user name.

User ID log of an SSH session established by SFTP

The switch logs the user ID of an SSH session initiated by SFTP. If SFTP establishes an SSH session, the message appears in the following format:

```
CP1  [08/06/15 09:45:32.903:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH user
authentication succeeded for user rwa on host 10.68.231.194
CP1  [08/06/15 09:45:32.905:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SFTP session
start: user rwa on host 10.68.231.194
CP1  [08/06/15 09:45:46.775:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SFTP session
closed by  user rwa on host 10.68.231.194
CP1  [08/06/15 09:45:46.776:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH SFTP
session end: user rwa on host 10.68.231.194
CP1  [08/06/15 09:45:46.776:UTC] 0x000d8602 00000000 GlobalRouter SSH INFO SSH session
closed by server for user rwa on host 10.68.231.194
```

In the preceding example log output, rwa is the user name.

User key files

Generating keys requires that you have free space on the flash. A typical configuration requires less than 2 kbyte of free space. Before you generate a key, verify that you have sufficient space on the flash, using the **dir** command. If the flash is full when you attempt to generate a key, an error message appears and the key is not generated. You must delete some unused files and regenerate the key.

If you remove only the public keys, enabling the SSH does not create new public keys.

SSHv2 password authentication uses the same login and password authentication mechanism as Telnet. The SSHv2 client also supports DSA public key authentication compatible with the switch SSHv2 server and Linux SSHv2 server for SSHv2.

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

Table 11: DSA user key files

SSH server	SSH client side	SSH server side
switch with enhanced secure mode disabled	Private and public keys by access level: • rwa—/intflash/.ssh/id_dsa_rwa (private key), /intflash/.ssh/id_dsa_rwa.pub (public key) • rw—/intflash/.ssh/id_dsa_rw (private key), /intflash/.ssh/id_dsa_rw.pub (public key) • ro—/intflash/.ssh/id_dsa_ro (private key), /intflash/.ssh/id_dsa_ro.pub (public key) • rwl1—/intflash/.ssh/id_dsa_rwl1 (private key), /intflash/.ssh/id_dsa_rwl1.pub (public key) • rwl2—/intflash/.ssh/id_dsa_rwl2 (private key), /intflash/.ssh/id_dsa_rwl2.pub (public key) • rwl3—/intflash/.ssh/id_dsa_rwl3 (private key), /intflash/.ssh/id_dsa_rwl3.pub (public key)	Public keys on the server side based on access level: • rwa—/intflash/.ssh/dsa_key_rwa (public key) • rw—/intflash/.ssh/dsa_key_rw (public key) • ro—/intflash/.ssh/dsa_key_ro (public key) • rwl1—/intflash/.ssh/dsa_key_rwl1 (public key) • rwl2—/intflash/.ssh/dsa_key_rwl2 (public key) • rwl3—/intflash/.ssh/dsa_key_rwl3 (public key)
switch with enhanced secure mode enabled	Private and public keys by access role level: • administrator—/intflash/.ssh/id_dsa_admin (private key), /intflash/.ssh/id_dsa_admin.pub (public key) • operator —/intflash/.ssh/id_dsa_operator (private key), /intflash/.ssh/id_dsa_operator.pub (public key) • security —/intflash/.ssh/id_dsa_security (private key), /intflash/.ssh/id_dsa_security.pub (public key) • auditor —/intflash/.ssh/id_dsa_auditor (private key), /intflash/.ssh/id_dsa_auditor.pub (public key)	Public keys on the server side based on access level: • administrator—/intflash/.ssh/dsa_key_admin (public key) • operator—/intflash/.ssh/dsa_key_operator (public key) • security—/intflash/.ssh/dsa_key_security (public key) • pirivilege—/intflash/.ssh/dsa_key_priv (public key) • auditor—/intflash/.ssh/dsa_key_auditor (public key)

Table continues…

SSH server	SSH client side	SSH server side
	• privilege —/intflash/.ssh/id_dsa_priv (private key), /intflash/.ssh/id_dsa_priv.pub (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)

When you attempt to make an SSH connection from the switch, the SSHv2 client looks in its own internal flash for the public key pair files. If the key files exist, the SSHv2 client prompts you for the passphrase to decrypt the key files. If the passphrase is correct, the SSHv2 client initiates the DSA key authentication to the remote SSHv2 server. The SSHv2 client looks for the login user access level public key file on the SSHv2 server to process and validate the public key authentication. If the DSA authentication is successful, then the SSHv2 session is established.

If no matching user key pair files exist on the client side when initiating the SSHv2 session, or if the DSA authentication fails, you are automatically prompted for a password to attempt password authentication.

If the remote SSHv2 server is a Linux system, the server looks for the login user public key file ~/.ssh/authorized_keys by default for DSA authentication. For a Linux SSHv2 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.

SCP command

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. The switch supports incoming SCP connections but does not support outgoing connections using an SCP client.

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 the switch software.

Table 12: Tested software

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)

Tera Term Pro with TTSSH extension
 	
MS Windows
	• Supports SSHv2.
	• Authentication:
	  - RSA is supported when the switch acts as a server. The switch does not support RSA as a client.
	  - DSA
	  - Password
	• Provides a keygen tool.
	• It creates both RSA and DSA keys.
		• Client distribution does not include SCP client.

Secure Shell Client
 	
Windows 2000
	• Supports SSHv2 client.
	• Authentication
	  - DSA
	  - Password
	• Provides a keygen tool.
	• It creates a DSA key in SSHv2 format.
	• The switch generates a log message stating that a DSA key has been generated.
		• Client distribution includes an SCP client that is not compatible with switch.

OpenSSH
Unix Solaris 2.5 / 2.6
	• Supports SSHv2 clients.
	• Authentication:
	  - RSA is supported when the switch acts as a server. The switch does not support RSA as a client.
	  - DSA
	  - Password
	• Provides a keygen tool.
	• It creates both RSA and DSA keys.
		• Client distribution includes an SCP client that is supported on switch.

WinSCP	N/A	This SCP client is unsupported on the switch.

Switch as client:

The switch acting as the SSHv2 client generates a DSA public and private server key pair. The public part of the key for DSA is stored in the following location:

`/intflash/.ssh/dsa_key_rwa`

The public part of the key must be copied to the SSH server and be named according to the naming requirement of the server.

Consult Table 13: DSA authentication access levels and file names on page 223 for proper naming convention.

If a DSA key pair does not exist, you can generate the DSA key pair using the **`ssh dsa-user-key [WORD<1–15>] [size <512-1024>]`** command.

You need to copy the DSA public key to the SSHv2 server that you connect to using the switch as a client. RSA is not supported when using the switch as a client, but you can use RSA when the switch is acting as the server.

Switch as server:

After you install one of the SSHv2 clients you must generate a client and server key using the RSA or DSA algorithms.

To authenticate an SSHv2 client using DSA, the administrator must copy the public part of the client DSA key to /intflash/.ssh directory on the switch that acts as the SSHv2 server. The file that is copied over to the SSHv2 server must be named according to Table 13: DSA authentication access levels and file names on page 223.

DSA authentication access level and file name

The following table lists the access levels and file names that you must use to store the SSHv2 client authentication information using DSA onto the switch that acts as the SSHv2 server.

Table 13: DSA authentication access levels and file names

Client key format or WSM	Access level	File name
Client key in non IETF and IETF format with enhanced secure mode disabled **Note:** ⊛ The switch supports IETF and non-IETF for DSA.	RWA	/intflash/.ssh/dsa_key_rwa
	RW	/intflash/.ssh/dsa_key_rw
	RO	/intflash/.ssh/dsa_key_ro
	L3	/intflash/.ssh/dsa_key_rwl3
	L2	/intflash/.ssh/dsa_key_rwl2
	L1	/intflash/.ssh/dsa_key_rwl1
Client key in enhanced secure mode	administrator	/intflash/.ssh/dsa_key_admin
	operator	/intflash/.ssh/dsa_key_operator
	security	/intflash/.ssh/dsa_key_security
	privilege	/intflash/.ssh/dsa_key_priv
	auditor	/intflash/.ssh/dsa_key_auditor

The switch 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 the switch

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 the switch.

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 14: RSA authentication access levels and file names

Client key format or WSM	Access level	File name
Client key in IETF format with enhanced secure mode disabled.	RWA	/flash/.ssh/rsa_key_rwa
	RW	/flash/.ssh/rsa_key_rw
	RO	/flash/.ssh/rsa_key_ro
	L3	/flash/.ssh/rsa_key_rwl3
	L2	/flash/.ssh/rsa_key_rwl2
	L1	/flash/.ssh/rsa_key_rwl1
Client key with enhanced secure mode enabled	administrator	/intflash/.ssh/rsa_key_admin
	operator	/intflash/.ssh/rsa_key_operator
	security	/intflash/.ssh/rsa_key_security
	privilege	/intflash/.ssh/rsa_key_priv
	auditor	/intflash/.ssh/rsa_key_auditor

SSL certificate

The switch 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. The system does not confirm if the certificate is still valid. If no certificate exists, then the system generates a default certificate (host.cert and also the key file, host.key) with a validity period of 365 days.

The switch uses the Avaya SSL certificate by default.

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. Restart the system and the new certificate will be loaded during the boot-up process.

> ❗ **Important:**
>
> Ensure that your certificate is PEM encoded with the appropriate header and footer. The switch does not support any other certificate encoding format.

Alternatively, you can use the `ssl certificate reset` command to install an existing certificate without a system reboot.

You can also use the `ssl certificate [validity-period-in-days <30-3650>]` command to install a new certificate and optionally, define an expiration date. You do not need to restart the system after you use this command.

The system does not validate the expiration date on the certificate and performs no action after the certificate expires. To confirm the expiration date, you must use Microsoft Internet Explorer or

Mozilla Firefox to view the certificate. If you cannot connect to the switch using HTTPS and the web portal displays a message of invalid certificate, that is an indication that the certificate on the switch is expired. You can replace the host.cert and host.key files with new files generated off the switch, or you can use the procedure to generate a new certificate on the switch with a specific validity period.

The default certificate key length for a certificate generated on the switch is 2,048 bits.

User configurable SSL certificates

If you generate a certificate on the switch, you can configure only the expiration time.

If you need to configure other user parameters, you can generate a certificate off the switch and upload the key and certificate files to the /intflash/ssh directory. Rename the uploaded files to host.cert and host.key, and then reboot the system. The system loads the user-generated certificates during startup. If the system cannot find host.cert and host.key during startup, it generates a default certificate.

The maximum supported size for user-configured SSL certificates is 4,096 bits.

SSH rekeying

SSH rekeying is an SSHv2 feature that allows the SSH server or client to force a key exchange between server and client, while changing the encryption and integrity keys. After you enable SSH rekeying, key exchanges occur after a pre-determined time interval or after the data transmitted in the session reaches the data-limit threshold. The default time-interval is 1 hour and the default data-limit is 1 GB. You can configure these values using the `ssh rekey` command.

SSH rekey is optional. You can enable SSH rekey only when SSH is enabled globally. Most SSH clients and servers do not provide a rekey mechanism, do not enable SSH rekey in such cases. Active sessions shut down if the rekey fails.

⊛ **Note:**

You cannot enable SSH rekey selectively for either SSH client or server, it is enabled both on the SSH client and server together.

Secure Shell configuration using CLI

Use Secure Shell version 2 (SSHv2) to enable secure communications support over a network for authentication, encryption, and network Integrity.

On IPv6 networks, the switch supports SSHv2 server only. The switch does not support outbound SSHv2 client over IPv6. On IPv4 networks, the switch supports both SSHv2 server and SSHv2 client.

Before you begin

- Disable the sshd daemon. All SSHv2 commands, except enable, require that you disable the sshd daemon.

- Set the user access level to read/write/all community strings.

- Disable all nonsecure access services. It is recommended 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 <u>Enabling remote access services</u> on page 59.

- Use the console port to configure the SSHv2 parameters. Depending on your hardware platform, the console port displays as console or 10101.

Downloading the software

Download new software to upgrade the switch.

Before you begin

- You must have access to the new software from the Avaya support site: <u>https:// support.avaya.com</u>. You need a valid user or site ID and password.

About this task

For more information about file names for the current release, see *Release Notes*.

Procedure

1. From an Internet browser, browse to <u>https://support.avaya.com</u>.

2. Under **Support by Product**, select **Downloads**.

3. In the product search field, type the product name.

4. In the **Choose Release** field, click a release number.

5. Click the download title to view the selected information.

6. Click the file you want to download.

7. Login to download the required software file.

8. Use an FTP client in binary mode to transfer the file to the switch.

Enabling the SSHv2 server

Enable the SSHv2 server to provide secure communications for accessing the switch. The switch does not support SSHv1.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

    `configure terminal`

2. Enable the SSH server:

    `boot config flags sshd`

3. Save the configuration file:

    `save config`

Example

Enable the SSHv2 server:

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

Changing the SSH server authentication mode

Use this procedure to change the SSH server authentication mode from the default of password-authentication to keyboard-interactive.

About this task

If you enable keyboard-interactive authentication mode, the server uses that mode over other authentication methods, except for public-key authentication, if the SSH client supports it.

If you enable keyboard-interactive authentication mode, the server generates the password prompts to display to the client rather than the client generating the prompts automatically like with password-authentication.

If you enable the ASG feature, you must change the SSH server to use keyboard-interactive authentication mode.

Procedure

1. Enter Global Configuration mode:

    `enable`

    `configure terminal`

2. Enable keyboard-interactive authentication:

    `ssh keyboard-interactive-auth`

Setting SSH configuration parameters

Configure Secure Shell version 2 (SSHv2) parameters to support public and private key encryption connections. The switch does not support SSHv1.

Before you begin

You must enable SSH globally before you can generate SSH DSA user keys.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable DSA authentication:

   ```
   ssh dsa-auth
   ```

3. Generate a new DSA host key:

   ```
   ssh dsa-host-key [<512-1024>]
   ```

4. Generate a new SSH DSA user key:

   ```
   ssh dsa-user-key WORD<1-15>
   ```

5. Configure the maximum number of SSH sessions:

   ```
   ssh max-sessions <0-8>
   ```

6. Enable password authentication:

   ```
   ssh pass-auth
   ```

7. Configure the SSH connection port:

   ```
   ssh port <22,1024..49151>
   ```

8. Enable RSA authentication:

   ```
   ssh rsa-auth
   ```

9. Generate a new RSA host key:

   ```
   ssh rsa-host-key [<1024-2048>]
   ```

10. Enable SSH secure mode:

    ```
    ssh secure
    ```

11. Configure the authentication timeout:

    ```
    ssh timeout <1-120>
    ```

12. Configure the SSH version:

    ```
    ssh version <v2only>
    ```

13. Enabling SSH rekey:

    ```
    ssh rekey data-limit <1-6>
    ```

    ```
    ssh rekey time-interval <1-6>
    ```

    ```
    ssh rekey enable
    ```

Example

Enable DSA authentication and configure the maximum number of SSH session:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ssh dsa-auth
Switch:1(config)#ssh max-sessions 5
```

Variable definitions

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

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>*	Generates a new SSH DSA user key. WORD<1–15> specifies the user access level. You must enable SSH globally before you can generate SSH DSA user keys. If enhanced secure mode is disabled, the valid user access levels for the switch 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. If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role. If enhanced secure mode is enabled, the valid user access levels for the switch are: • admin—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles. • operator—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands. • auditor—Specifies a user role that can view log files and view all configurations, except password configuration.

Table continues…

Variable	Value
	• security—Specifies a user role with access only to security settings and the ability to view the configurations.
	• priv—Specifies a user role with access to all of the commands that the administrator has access to, and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only.
	Use the no operator before this parameter, `no ssh dsa-user-key WORD<1-15>`, 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.
pass-auth	Enables password authentication. The default is enabled.
port *<22,1024–49151>*	Configures the Secure Shell (SSH) connection port. *<22,1024 to 49151>* is the TCP port number. The default is 22 **❶ Important:** You cannot configure TCP port 6000 as the SSH connection port.
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 *[<1024–2048>]*	Generates a new SSH RSA host key. Specify an optional key size from 1024 to 2048. The default is 2048. 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>*	Configures the SSH version. The default is v2only. The switch only supports SSHv2.

Verifying and displaying SSH configuration information

Verify that SSH services are enabled on the switch and display SSH configuration information to ensure that the SSH parameters are properly configured.

Procedure

1. Log on to the switch to enter User EXEC mode.

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

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

Example

Display global system SSH information:

```
Switch:1>show ssh global

Total Active Sessions  : 0
        version                 : v2only
        port                    : 22
        max-sessions            : 4
        timeout                 : 60
        action rsa-host key     : rsa-hostkeysize 2048
        action dsa-host key     : dsa-hostkeysize 1024
        rsa-auth                : true
        dsa-auth                : true
        pass-auth               : true
        keyboard-interactive-auth : false
        sftp enable             : true
        enable                  : true
        client enable           : true
```

Variable definitions

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

Variable	Value
global	Display global system SSH information.
session	Display the current session SSH information.

Connecting to a remote host using the SSH client

Make an SSH connection to a remote host.

Before you begin

Enable the SSH server on the remote host.

About this task

The command format, for the CLI SSH client command, is similar to Telnet with two additional parameters: -l login and an optional -p port parameter.

On IPv6 networks, the switch supports SSH server only. The switch does not support outbound SSH client over IPv6. On IPv4 networks, the switch supports both SSH server and SSH client.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Connect to a remote host:

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

Example

Connect to the remote host:

```
Switch:1>enable
Switch:1#ssh 192.0.2.1 -l rwa
```

Variable definitions

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

Variable	Value
WORD<1–32>	Specifies the user login name of the remote SSH server.
-p <1-32768>	Specifies the port number to connect to the remote SSH server. The default is 22.

Generating user key files

Configure the SSH parameters to generate DSA user key files.

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal

2. Enable SSH server.

3. Create the DSA user key file:

   ssh dsa-user-key *[WORD<1–15>]*[size *<512–1024>*]

4. Enter the encryption password to protect the key file.

5. Copy the user public key file to the remote SSH servers.

6. If you are generating the compatible keys on a Linux system, use the following steps:

   a. Create the DSA user key file:

      ssh-keygen –t dsa

   b. Copy the user public key to the remote SSH servers.

      ⊛ **Note:**

      The DSA pair key files can be generated on the Linux system and used by the SSH client on the switch.

Example

Create the DSA user key file with the user access level set to read-write-all and size of the DSA user key set to 512 bits:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ssh dsa-user-key rwa size 512
```

Variable definitions

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

Variable	Value
WORD<1–15 >	Specifies the user access level. If enhanced secure mode is disabled, the valid user access levels for the switch 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.
	If you enable enhanced secure mode, the switch uses role-based authentication. You associate each username with a specific role and the appropriate authorization rights to commands based on that role.
	If enhanced secure mode is enabled, the valid user access levels for the switch are:
	• admin—Specifies a user role with access to all of the configurations, show commands, and the ability to view the log file and security commands. The administrator role is the highest level of user roles.
	• operator—Specifies a user role with access to all of the configurations for packet forwarding on Layer 2 and Layer 3, and has access to show commands to view the configuration, but cannot view the audit logs and cannot access security and password commands.
	• auditor—Specifies a user role that can view log files and view all configurations, except password configuration.
	• security—Specifies a user role with access only to security settings and the ability to view the configurations.
	• priv—Specifies a user role with access to all of the commands that the administrator has access to,

Table continues…

Variable	Value
	and is referred to as an emergency-admin. However, the user with the privilege role must be authenticated within the switch locally. RADIUS and TACACS+ authentication is not accessible. A user role at the privilege level must login to the switch through the console port only.
size *<512–1024>*	Specifies the size of the DSA user key. The default is 1024 bits.

Managing an SSL certificate

Perform this procedure to manage an SSL certificate on the switch.

About this task

If a certificate is already present, you must confirm that it can be deleted before a new one is created.

After you create a certificate, the system logs one of the following INFO alarms:

- `New default Server Certificate and Key are generated and installed`
- `Current Server Certificate and Key are installed`

The default certificate key length for a certificate generated on the switch is 2,048 bits.

✳ Note:

The `ssl certificate [validity-period-in-days <30-3650>]` command in this procedure does not require a system reboot.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create and install a new self-signed certificate:

   ```
   ssl certificate [validity-period-in-days <30-3650>]
   ```

3. Delete a certificate:

   ```
   no ssl certificate
   ```

   ✳ Note:

   The certificate loaded in memory remains valid until you use the `ssl reset` command or reboot the system.

Variable definitions

Use the data in the following table to use the `ssl certificate` command.

Variable	Value
validity-period-in-days <30-3650>	Specifies an expiration time for the certificate. The default is 365 days.

Disabling SFTP without disabling SSH

Disable SFTP while allowing SSH to remain active.

Before you begin

Enhanced secure mode must be enabled. For information about enabling enhanced secure mode, see Enabling enhanced secure mode on page 262.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable the SSHv2 server:

   ```
   no ssh sftp enable
   ```

3. Save the configuration file:

   ```
   save config
   ```

Enabling SSH rekey

Before you begin

Enable SSH globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command:

   ```
   ssh rekey enable
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Enable SSH rekeying globally:

```
Switch:1(config)#ssh rekey enable
```

Variable Definitions

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

Variable	Value
enable	Enables SSH rekey globally.

Configuring SSH rekey data-limit

Use the following procedure to configure the limit for data transmission during the session.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command:

   ```
   ssh rekey data-limit <1-6>
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Configure the SSH rekey data-limit to 2 GB:

```
Switch:1(config)#ssh rekey data-limit 2
```

Variable definitions

Use the following table to use the `ssh rekey data-limit` command.

Variable	Value
<1–6>	Sets the SSH rekey data limit in GB, range is 1–6.

Configuring SSH rekey time-interval

Use the following procedure to configure a time interval, after which the key exchange takes place.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command:

   ```
   ssh rekey time-interval <1-6>
   ```

Example

```
Switch:1> enable
Switch:1# configure terminal
```

Configure the SSH rekey time-interval to 3 hours:

```
Switch:1(config)# ssh rekey time-interval 3
```

Variable definitions

Use the data in the following table to use the **ssh rekey time-interval** command.

Variable	Value
<1–6>	Sets the time-interval for SSH rekeying in hours, the range is 1 to 6.

Displaying SSH rekey information

Use the following procedure to display the SSH rekey information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command:

   ```
   show ssh rekey
   ```

Example

```
Switch:1> enable
Switch:1#show ssh rekey
       Rekey Status       : TRUE
       Rekey data limit   : 1 GB
       Rekey time interval : 1 hours
```

Field descriptions

The following table describes the output for the **show ssh rekey** command.

Name	Description
Rekey status	Displays the status (TRUE or FALSE) of SSH rekeying.
Rekey data limit	Displays the configured SSH rekey data transmission limit GB.
Rekey time interval	Displays the configured SSH rekey time interval in hours.

Enabling or disabling the SSH client

About this task

You can disable the SSH client functionality on the switch. By default, the SSH client functionality is enabled.

* **Note:**

    In order to enable the SSH client functionality, SSH must be enabled globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Disable the SSH client functionality:

   ```
   no ssh client <enable>
   ```

3. Use one of the following commands to enable the SSH client functionality:

   - `ssh client <enable>`

   - `default ssh client <enable>`

   * **Note:**

       You must enable SSH globally before the SSH client functionality can be re-enabled.

Example

Display the general SSH settings::

```
Switch:1(config)# show ssh global
```

```
Total Active Sessions  :  0
        version               : v2only
        port                  : 22
        max-sessions          : 4
        timeout               : 60
        action rsa-host key   : rsa-hostkeysize 2048
        action dsa-host key   : dsa-hostkeysize 1024
        rsa-auth              : true
        dsa-auth              : true
        pass-auth             : true
        keyboard-interactive-auth : false
        sftp enable           : true
        enable                : true
        client enable         : true
```

Disable SSH client functionality:

```
Switch:1(config)# no ssh client
```

```
Switch:1(config)# show ssh global

Total Active Sessions  :  0
        version              : v2only
        port                 : 22
        max-sessions         : 4
        timeout              : 60
        action rsa-host key  : rsa-hostkeysize 2048
        action dsa-host key  : dsa-hostkeysize 1024
        rsa-auth             : true
        dsa-auth             : true
        pass-auth            : true
        keyboard-interactive-auth : false
        sftp enable          : true
        enable               : true
        client enable        : false
```

Secure Shell configuration using Enterprise Device Manager

Use Secure Shell version 2 (SSHv2) to enable secure communications support over a network for authentication, encryption, and network Integrity.

On IPv6 networks, the switch supports SSHv2 server only. The switch does not support outbound SSHv2 client over IPv6. On IPv4, the switch supports both SSHv2 server and SSHv2 client.

For more information, see

For information about downloading and enabling security encryption, see

Downloading the software

Download new software to upgrade the switch.

Before you begin

* You must have access to the new software from the Avaya support site: https://support.avaya.com. You need a valid user or site ID and password.

About this task

For more information about file names for the current release, see *Release Notes*.

Procedure

1. From an Internet browser, browse to https://support.avaya.com.

2. Under **Support by Product**, select **Downloads**.

3. In the product search field, type the product name.

4. In the **Choose Release** field, click a release number.

5. Click the download title to view the selected information.

6. Click the file you want to download.

7. Login to download the required software file.

8. Use an FTP client in binary mode to transfer the file to the switch.

Changing Secure Shell parameters

You can use Enterprise Device Manager to change the SSHv2 configuration parameters. However, it is recommended to use the CLI to perform the initial configuration of SSHv2. The switch does not support SSHv1.

Before you begin

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

- You must disable the SSH service before you configure the SSH service parameters. If the SSHv2 service is enabled, all fields appear dimmed until the SSH service is disabled.

Procedure

1. In the navigation pane, expand the **Configuration** > **Security** > **Control Path** folders.

2. Click **SSH**.

3. Click the **SSH** tab.

4. In the **Enable** field, select the type of SSH service you want to enable.

5. In the **Version** field, select a version.

6. In the **Port** field, type a port.

7. In the **MaxSession** field, type the maximum number of sessions allowed.

8. In the **Timeout** field, type the timeout.

9. From the **KeyAction** field, choose a key action.

10. In the **RsaKeySize** field, type the RSA key size.

11. In the **DSAKeySize** field, type the DSA key size.

12. Select the **RsaAuth** check box for RSA authentication.

13. Select the **DsaAuth** check box for DSA authentication.

14. Select the **PassAuth** check box for password authentication.

15. 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 SSHv2. The options are: • false • true • secure Select false to disable SSHv2 services. Select true to enable SSHv2 services. Select secure to enable SSH and disable access services (SNMP, FTP, TFTP, rlogin, and Telnet). The default is false. ❗ **Important:** Do not enable SSHv2 secure mode using Enterprise Device Manager. Enabling secure mode disables SNMP. This locks you out of the Enterprise Device Manager session. Enable SSHv2 secure mode using CLI.
Version	Configures the SSH version. The options are: • v2only The default is v2only.
Port	Configures the SSHv2 connection port number. *<22 or 1024–49151>* is the port range of SSHv2. ❗ **Important:** You cannot configure the TCP port 6000 as SSHv2 connection port.
MaxSession	Configures the maximum number of SSHv2 sessions allowed. The value can be from 0 to 8. The default is 4.
Timeout	Configures the SSHv2 authentication connection timeout in seconds. The default is 60 seconds.
KeyAction	Configures the SSHv2 key action. The options are: • none • generateDsa • generateRsa • deleteDsa • deleteRsa
RsaKeySize	Configures SSHv2 RSA key size. The value can be from 1024 to 2048. The default is 2048.
DsaKeySize	Configures the SSHv2 DSA key size. The value can be from 512 to 1024. The default is 1024.
RsaAuth	Enables or disables SSHv2 RSA authentication. The default is enabled.
DsaAuth	Enables or disables SSHv2 DSA authentication. The default is enabled.
PassAuth	Enables or disables SSHv2 RSA password authentication. The default is enabled.

Table continues…

Name	Description
SftpEnable	Enables or disables SFTP. You can use this check box to disable SFTP without affecting the SSH status. The default is enabled.
KeyboardInteracti veAuth	Changes the SSH server authentication mode from the default of password authentication to keyboard interactive.

Chapter 16: System access

The following sections describe how to access the switch, create users, and user passwords.

System access fundamentals

This section contains conceptual information about how to access the switch and create users and user passwords for access.

Logging on to the system

After the startup sequence is complete, the login prompt appears.

⊛ **Note:**

With enhanced secure mode enabled, the person in the role-based authentication level of administrator configures the login and password values for the other role-based authentication levels. The administrator initially logs on to the switch using the default login of `admin` and the default password of `admin`. After the initial login, the switch prompts the administrator to create a new password.

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user. For more information on enhanced secure mode, see System access security enhancements on page 260.

The following table shows the default values for login and password for the console and Telnet sessions.

Table 15: 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

Table continues…

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

You can enable or disable users with particular access levels, eliminating the need to maintain large numbers of access levels and passwords for each user.

The system denies access to a user with a disabled access level who attempts to log on. The following error message appears after a user attempts to log on with a blocked access level:

```
CPU1 [mm/dd/yy hh:mm:ss] 0x0019bfff GlobalRouter CLI WARNING Slot 1: Blocked unauthorized
cli access
```

The system logs the following message to the log file:

```
User <user-name> tried to connect with blocked access level <access-level> from <src-
ipaddress> via <login type>.
```

The system logs the following message for the console port:

```
User <user-name> tried to connect with blocked access level <access-level> from console
port.
```

RADIUS authentication

Remote Authentication Dial-in User Service (RADIUS) authentication takes precedence over the local configuration. If you enable RADIUS authentication on the switch, the user can access the switch even if you block an access level on the switch.

> ❗ **Important:**
>
> When you enable RADIUS on the switch and configure a RADIUS server to be used by CLI or EDM, the server authenticates the connection, whether it is FTP, HTTPS, SSH, or TELNET. However, in the event that the RADIUS server is unresponsive or is unreachable, the switch will fall back to the local authentication, so that you can access the switch using your local login credentials.

If you disable an access level, all running sessions, except FTP sessions, with that access level to the switch terminate.

> ❗ **Important:**
>
> Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.
>
> The system preserves these configurations across restarts.

hsecure bootconfig flag

The switch 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 *Configuring Security*.

Enhanced secure mode

If you enable enhanced secure mode, the system uses different authentication levels. Enhanced secure mode allows the system to:

- Provide role-based access levels
- Stronger password requirements
- Stronger rules on password length
- Stronger rules on password complexity
- Stronger rules on password change intervals
- Stronger rules on password reuse
- Stronger password maximum age use

For more information on enhanced secure mode, see System access security enhancements on page 260.

Managing the system using different VRF contexts

You can use the Enterprise Device Manager (EDM) to manage the system using different Virtual Router Forwarding (VRF) contexts.

- Using the GlobalRouter (VRF 0), you can manage the entire system. GlobalRouter is the default view at log in

- Using a VRF context other than the GlobalRouter (VRF 0), you have limited functionality to manage the system. For instance you can only manage the ports assigned to the specified VRF instance

Specify the VRF instance name on the EDM screen when you launch a VRF context view. You can use the context names (SNMPv3) and community strings (SNMPv1/v2) to assign different VRFs to manage selected components, such as ports and VLANs. For more information about context names and community strings, see *Configuring Security*.

CLI passwords

The switch ships with default passwords configured for access to CLI 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. Change the default passwords and community strings immediately after the first logon.

For security, if you fail to log on correctly in three consecutive instances, then the device locks for 60 seconds.

The switch 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 the switch, 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 the switch (ro, l1, l2, l3, rw, rwa)

- Command access (single instance)–indicates whether the user has access to the commands on the RADIUS server

- CLI commands (multiple instances)–the list of commands that the user can or cannot use

Access policies for services

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), Secure Shell version 2 (SSHv2), and remote login (rlogin). You can enable or disable access services by configuring flags.

Use access policies for in-band management to secure access to the switch. By default, all services are denied. You must enable the default policy or enable a custom policy to provide access. A lower precedence takes higher priority if you use multiple policies. Preference 120 has priority over preference 128.

You can define network stations that can access the switch or stations that cannot access the switch. For each service you can also specify the level of access, such as read-only or read-write-all.

When you configure access policies, you can perform either of the following actions:

- Globally enable the access policy feature, and then create and enable individual policies. Each policy takes effect immediately after you enable it.

- Create and enable individual access policies, and then globally enable the access policy feature to activate all the policies at the same time.

HTTP, SSH and rlogin support IPv4 and IPv6 with no difference in configuration or functionality.

Web interface passwords

The switch includes a Web-management interface, Enterprise Device Manager (EDM), that you can use to monitor and manage the device through a supported Web browser from anywhere on the network. For more information on supported web browsers, see *Using CLI and EDM*.

A security mechanism protects EDM and requires you to log on to the device using a user name and password. The default user name is `admin` and the default password is `password`.

> ❗ **Important:**
>
> For security reasons, EDM is disabled by default. For instructions about how to enable the interface, see *Quick Start Configuration*.

Password encryption

The switch handles password encryption in the following manner:

- After the device starts, the system restores the web-server passwords and community strings from the hidden file.

- After you modify the web-server username and password or SNMP community strings, the system makes the modifications to the hidden file.

Enhanced secure mode authentication access levels

After you enable enhanced secure mode with the `boot config flags enhancedsecure-mode` command, the switch supports role-based authentication levels. With enhanced secure mode enabled, the switch supports the following authentication access levels for local authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

Each username is associated with a certain role in the product and appropriate authorization rights for viewing and executing commands are available for that role.

With enhanced secure mode enabled, the person in the role-based authentication level of administrator configures the login and password values for the other role-based authentication levels.

The administrator initially logs on to the switch using the default login of `admin` and the default password of `admin`. After the initial login, the switch prompts the administrator to create a new password.

The following displays an example of the initial login to the switch by the administrator after enhanced secure mode is enabled.

```
Login: admin
Password: *****
        This is an initial attempt using the default user name and password.
        Please change the user name and password to continue.
Enter the new name : rwa
Enter the New password : ****************
Re-enter the New password : ****************
Password changed successfully
        Last Successful Login:Wed Oct 14 12:20:42 2015
         Unsuccessful Login attempts from last login is: 0
```

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user.

Access level and login details

Access level	Description	Login location
Administrator	The administrator access level permits all read-write access, and can change security settings. The administrator access level can	SSH/Telnet (in band/mgmt)/ console

Table continues…

Access level	Description	Login location
	configure CLI and web-based management user names, passwords, and the SNMP community strings. The administrator access level can also view audit logs.	
Privilege	The privilege access level has the same access permission as the administrator; however, the privilege access level cannot use RADIUS or TACACS+ authentication. The system must authenticate the privilege access level within the switch at a console level. The privilege access level is also known as emergency-admin.	console
Operator	The operator access level can view most switch configurations and status information. The operator access level can change physical port settings at layer 2 and layer 3. The operator access level cannot access audit logs or security settings.	SSH/Telnet(in band/mgmt)/console/
Auditor	The auditor access level can view configuration information, status information, and audit logs.	SSH/Telnet(in band/mgmt)/console/
Security	The security access level can change security settings only. The security access level also has permission to view configuration and status information.	SSH/Telnet(in band/mgmt)/console/

Password requirements

After you enable enhanced secure mode on the switch the password requirements are stronger. The individual in the administrator access level role configures and provides a temporary user name and password. After you log in for the first time with the temporary user name and temporary password, the system forces you to change the temporary password. After you change the temporary password, you cannot use the password again in subsequent sessions.

The following topic discusses the enhanced password requirements.

Password complexity rule

After you enable enhanced secure mode, the system checks each password change request to ensure the new password meets the password complexity required.

The default for the password complexity rule includes the following:

- Two uppercase character, from the range: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Two lowercase character, from the range: abcdefghijklmnopqrstuvwxyz
- Two numeric character, from the range: 1234567890
- Two special character, from the range: `~!@#$%^&*()_-+={[}]|\:;"'<,>.?/

Password length rule

The system enforces a minimum password length of 15 characters after you enable enhanced secure mode.

If you do not meet the password length rule, the system displays the following message:

```
Password change aborted. The new password does not meet the minimum
complexity requirement. Please select another password that meets the
change interval, length, complexity, no consecutive repeating characters
or history requirements of the domain.
```

Password change interval rule

The system enforces a minimum password change interval, which defines the minimum amount of time before you can change to a new password. By default, the minimum change interval is 24 hours between changing from one password to a new password. If you want to change your password, and attempt to do so, the system checks the timestamp for your password to determine if enough time has passed to allow you to change the password.

If you attempt to change the password and not enough time has passed, the system rejects the request, and the system informs you that the password was recently changed. Any password change outside of the enforced interval requires the Administrator to approve the change.

If you try to change the password before the change interval allows, the system displays the following message:

```
Password change aborted. The new password does not meet the minimum
complexity requirement. Please select another password that meets the
change interval, length, complexity, no consecutive repeating characters
or history requirements of the domain.
```

Password reuse rule

After you enable enhanced secure mode, the administrator access level can define the number of old passwords that cannot be reused. The password reuse rule ensures that recently used passwords are not reused immediately, which reduces the risk of someone unlawfully gaining access to the system. The default number of prohibited recently used passwords is 3, but you can define up to 99.

The system saves the password history and stores the history in an encrypted format, along with the user name, and date of change. If a particular user attempts to change a password, the system looks up the password history list, and checks it against the stored passwords the user has previously used. If the password is on the list of previously used passwords, the system rejects the password change, and displays the following message:

```
Old password not allowed.
```

Password maximum age rule

The system enforces automatic password renewal and password lockout after the expiration period because long-term usage of the same password can cause the system to be vulnerable to hacking.

You can configure the password expiration period to a range of 1 to 365 days. The default password expiration period is 90 days.

Password max-session

The password max-sessions value indicates the maximum number of times a particular type of role-based user can log in to the switch through the SSH session at the same time. The max-sessions value applies only for SSH sessions, and only with enhanced secure mode enabled.

After the maximum session number is reached that particular type of user cannot login. For example, if the max-sessions for an auditor user is configured as 5, then the auditor user can log in to only five SSH sessions at the same time. The default is 3.

Password pre-notification interval and post-notification interval rule

After enhanced secure mode is enabled, the switch enforces password expiry. To ensure a user does not lose access, the switch offers pre- and post-notification messages explaining when the password will expire.

The administrator can define pre- and post-notification intervals to between one to 99 days.

The system maintains the password with a time stamp for when the password expiration. When you log in, the system checks the password time stamp and the notification timer values. If the administrator configures the pre-notification to 30 days, when you log in, the system checks the time stamp and notification timer values, and if the password expiry is due in 30 days, the system displays the first notification.

The pre-notification intervals provide messages to warn users that their passwords will expire within a particular timeframe:

- interval 1—By default, interval 1 is 30 days.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 1 day.

The post-notification intervals provide notification to users that their passwords have expired within a particular timeframe:

- interval 1—By default, interval 1 is 1 day.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 30 days.

If you do not change the password before the expiry date, the system locks your account. Once locked, only the administrator can unlock the account. The administrator creates a temporary password, and then you can login with the temporary password.

System access configuration using CLI

The section provides procedures to manage system access through configurations such as usernames, passwords, and access policies.

Enabling CLI access levels

Enable CLI access levels to control the configuration actions of various users.

About this task

🛇 **Important:**

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

The system preserves these configurations across restarts.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable an access level:

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

Example

Block CLI access to Layer 1:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no password access-level l1
```

Variable definitions

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

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.

Variable	Value
	• 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

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the switch, use default passwords to initially access CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Before you begin

- You must use an account with read-write-all privileges to change passwords. For security, the switch saves passwords to a hidden file.

About this task

If you enable the hsecure flag, after the aging time expires, the system prompts you to change your password. If you do not configure the aging time, the default is 90 days.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Change a password:

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

3. Enter the old password.

4. Enter the new password.

5. Enter the new password a second time.

6. Configure password options:

   ```
   password [access-level WORD<2-8>] [aging-time <1-365>] [default-
   lockout-time <60-65000>] [lockout WORD<0-46> time <60-65000>] [min-
   passwd-len <10-20>] [password-history <3-32>]
   ```

Example

Change a password, and then set the password to an access level of read-write-all and the expiration period for the password to 60 days:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#cli password smith read-write-all
Switch:1(config)#Enter the old password : winter
Switch:1(config)#Enter the New password : summer
Switch:1(config)#Re-enter the New password : summer
Switch:1(config)#password access-level rwa aging-time 60
```

Variable definitions

Use the data in the following table to use the `cli password` command.

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.

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.

Table continues…

Variable	Value
	• *<60-65000>* is the lockout-out time, in seconds, in the 60–65000 range. The default is 60 seconds.
min-passwd-len *<10-20>*	Configures the minimum length for passwords in high-secure mode. The default is 10 characters.
	To configure this option to the default value, use the default operator with the command.
password-history *<3-32>*	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default is 3.
	To configure this option to the default value, use the default operator with the command.

Configuring an access policy

About this task

Configure an access policy to control access to the switch.

You can permit network stations to access the switch or forbid network stations to access the switch.

For each service, you can also specify the level of access; for example, read-only or read-write-all.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Create an access policy by assigning it a number:

   `access-policy <1-65535>`

3. Restrict the access to a specific level:

   `access-policy <1-65535> access-strict`

4. Configure access for an access policy:

   `access-policy <1-65535> accesslevel <ro|rwa|rw>`

5. Configure the access policy mode, network, and precedence:

   `access-policy <1-65535> [mode <allow|deny>] [precedence <1-128>] [network <A.B.C.D> <A.B.C.D>]`

   If you configure the access policy mode to **deny**, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to **deny**, the system does not check **accesslevel** and **access-strict** information. If you

configure the access policy mode to allow, the system continues to check the `accesslevel` and `access-strict` information.

6. **(Optional)** Configure access protocols for an access policy:

   `access-policy <1-65535> [ftp] [http] [ssh] [telnet] [tftp]`

7. **(Optional)** Configure trusted username access for an access policy:

   `access-policy <1-65535> host WORD<0-46> [username WORD<0-30>]`

8. **(Optional)** Configure SNMP parameters for an access policy:

   `access-policy <1-65535> [snmp-group WORD<1-32> <snmpv1|snmpv2c|usm>]`

   OR

   `access-policy <1-65535> [snmpv3]`

9. Enable the access policy:

   `access-policy <1-65535> enable`

10. Enable access policies globally:

    `access-policy`

Example

Assuming no access policies exist, start with policy 3 and name the policy policy3. Add the read-write-all access level and the usm group group_example. Enable access strict, and finally, enable the policy.

```
Switch:1(config)#access-policy 3
Switch:1(config)#access-policy 3 name policy3
Switch:1(config)#access-policy 3 accesslevel rwa
Switch:1(config)#access-policy 3 snmp-group group_example usm
Switch:1(config)#access-policy 3 access-strict
Switch:1(config)#access-policy 3 enable
```

Variable definitions

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

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.

Table continues…

Variable	Value
enable	Enables the access policy.
ftp	Activates or disables FTP for the specified policy. Because FTP derives its login and password from the CLI management filters, FTP works for read-write-all (rwa) and read-write (rw) access, but not for the read-only (ro) access. Use the no operator to remove this configuration.
host *WORD<0–46>*	For remote login access, specifies the trusted host address as an IP address. The switch supports access-policies over IPv4 and IPv6 with no difference in 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. If you configure the access policy mode to deny, the system checks the mode and service, and if they match, the system denies the connection. With the access policy mode configured to deny, the system does not check accesslevel and access-strict information. If you configure the access policy mode to allow, the system continues to check the accesslevel and access-strict information.
name WORD<0-15>	Specifies the access policy name.
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. The switch supports access-policies over IPv4 and IPv6 with no difference in 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.
rlogin	Enables rlogin for the access policy.
snmp-group *WORD<1–32>* <snmpv1|snmpv2c|usm>	Adds an SNMP version 3 group under the access policy.

Table continues…

Variable	Value
	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.
	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

The policy must exist before you can name it.

About this task

Assign a name to an existing access policy to uniquely identify the policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Assign a name to the access policy:

   ```
   access-policy <1-65535> name WORD<0-15>
   ```

Example

Assign a name to an access policy:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#access-policy 10 name useraccounts
```

Variable definitions

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

Variable	Value
name WORD<0–15>	Specifies a name expressed as a string from 0–15 characters.

Allowing a network access to the switch

About this task

Specify the network to which you want to allow access.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Specify the network:

   ```
   access-policy <1-65535> [mode <allow|deny>] [network <A.B.C.D>
   <A.B.C.D>]
   ```

Example

Specify the network to which you want to allow access:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#access-policy 5 mode allow network 192.192.192.0 24
```

Variable definitions

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

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.
network <A.B.C.D> <A.B.C.D>	Specifies 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

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. Configuring access-policies by MAC address does not perform MAC or Forwarding Database (FDB) filtering on data ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Add the MAC address and configure the action for the policy:

   ```
   access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>
   ```

3. Specify the action for a MAC address that does not match the policy:

   ```
   access-policy by-mac action <allow|deny>
   ```

Example

Add the MAC address:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch: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.

Variable	Value
<0x00:0x00:0x00:0x00: 0x00:0x00>	Adds a MAC address to the policy. Enter the MAC address in hexadecimal format.
<allow|deny>	Specifies the action to take for the MAC address.

System access security enhancements

The section provides information on security enhancements after you enable enhanced secure mode.

Displaying the boot config flags status

Use the following procedure to display the boot config flags status.

If enhanced secure mode is enabled, the status displays whether the JITC or non-JITC sub-mode is enabled. If enhanced secure mode is disabled, the status displays as false.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. View the boot flag status:

   ```
   show boot config flags
   ```

Example

⭐ **Note:**

The ipv6-mode flag does not apply to all hardware models.

The status displays the sub-mode in which the enhanced secure mode is enabled, that is, either the JITC or non-JITC. In the following example, the status displays that the non-JITC sub-mode is enabled.

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags dvr-leaf-mode false
flags enhancedsecure-mode non-jitc
flags factorydefaults false
flags flow-control-mode false
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags nni-mstp true
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode false
flags verify-config true
flags vrf-scaling false
flags vxlan-gw-full-interworking-mode false
```

In the following example, the enhanced secure mode displays as false, which means the enhanced secure mode is disabled:

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags dvr-leaf-mode false
flags enhancedsecure-mode false
flags factorydefaults false
```

```
flags flow-control-mode false
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode false
flags verify-config true
flags vrf-scaling false
flags vxlan-gw-full-interworking-mode false
```

Enabling enhanced secure mode

Use the following procedure to enable enhanced secure mode. Enhanced secure mode is disabled by default.

About this task

⊛ **Note:**

When you migrate your switch from enhanced secure mode enabled to disabled, or from disabled to enabled, you must build a new configuration. Do not use a configuration created in either enhanced secure mode disabled or enabled, and expect it to transfer over to the new mode.

The configuration file cannot be guaranteed if you transfer between enhanced secure mode enabled to disabled, or from enhanced secure mode disabled to enabled.

After you enable the enhanced secure mode, the system provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use. The enhanced secure mode boot flag supports two sub-modes namely JITC and non-JITC.

After you disable enhanced secure mode, the authentication, access-level, and password requirements work similarly to any of the existing commercial releases.

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal

2. Enable enhanced secure mode:

   boot config flags enhancedsecure-mode [jitc | non-jitc]

> ✱ **Note:**
>
> It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode, because the JITC sub-mode is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting.

3. **(Optional)** Disable enhanced secure mode:

   ```
   no boot config flags enhancedsecure-mode
   ```

4. **(Optional)** Configure the enhanced secure mode to the default value:

   ```
   default boot config flags enhancedsecure-mode
   ```

5. Save the configuration:

   ```
   save config
   ```

   > ✱ **Note:**
   >
   > The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

6. Restart the switch:

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

   > ✱ **Note:**
   >
   > If you enter the `boot` command with no arguments, you cause the switch to start using the current boot choices defined by the `boot config choice` command.
   >
   > If you enter a boot command and the configuration filename without the directory, the device uses the configuration file from /intflash/.

Example

Enable the enhanced secure non-JITC sub-mode:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags enhancedsecure-mode non-jitc
Switch:1(config)#save config
Switch:1(config)#exit
Switch:1(config)#boot config /intflash/config.cfg -y
```

Enable the enhanced secure JITC sub-mode:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#boot config flags enhancedsecure-mode jitc
Switch:1(config)#save config
Switch:1(config)#exit
Switch:1(config)#boot config /intflash/config.cfg -y
```

Variable definitions

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

Variable	Value
jitc	Enables the JITC enhanced secure mode. The JITC mode is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting.
non-jitc	Enables the non-JITC enhanced secure mode.

Creating accounts for different access levels

Use the following procedure to create accounts for different access levels in enhanced secure mode. You must be the administrator to configure the different access levels.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create accounts on the switch for different access levels:

   ```
   password create-user {auditor|operator|privilege|security} WORD<1–255>
   ```

3. Save the configuration:

   ```
   save config
   ```

   > ⊛ **Note:**
   >
   > The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Create an account at the auditor level for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password create-user auditor jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password create-user** command.

Variable	Value
{auditor|operator|privilege|security}	Specifies the access level for the user.
WORD<1–255>	Specifies the user name.

Deleting accounts in enhanced secure mode

Use the following procedure to delete accounts in enhanced secure mode.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
- You must be an admin or privilege user to delete accounts.

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal

2. Delete an account on the switch:

   password delete-user *username WORD<1–255>*

3. Save the configuration:

   save config

   ⊛ **Note:**

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

Example

Delete an account for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password delete-user user-name jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password delete-user** command.

Variable	Value
user-name WORD<1–255>	Specifies the user name.

Configuring a password for a specific user

Configure a new password for a user if the password has expired or locked. Only the administrator can configure a password for a user.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create accounts on the switch for different access levels:

   ```
   password set-password user-name WORD<1-255>
   ```

3. Save the configuration:

   ```
   save config
   ```

   ⭐ **Note:**

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

Example

Configure a password for jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password set-password user-name jsmith
Enter the New password : *********************
Switch:1(config)#Password modified for user jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password set-password** command.

Variable	Value
user-name WORD<1–255>	Specifies the user for which to configure the password.

Returning the system to the factory defaults

Return the system to factory defaults. Reset the switch to the default passwords and configuration. If you use this command, the system returns to factory defaults, returns necessary flags to their default values, and deletes all of the configured user accounts in enhanced secure mode.

You can only access this command after you enable enhanced secure mode. Only the individual with the administrator access role can use this command. After the administrator uses this command, the administrator must reboot the switch.

> ✱ **Note:**
>
> The command `sys sys-default` does not save the config file. When you execute the command `sys sys-default`, you must reboot the system to have the command take effect. After the system reboots, you must login and then save the config file. Otherwise, if you reboot the device again for a second time without saving the config file, the changes are not saved and the system comes back up in enhanced secure mode.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
- Save the configuration to a file to retain the configuration settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Return the system to the factory defaults:

   ```
   sys system-default
   ```

3. Restart the switch:

   ```
   reset
   ```

4. Save the configuration:

   ```
   save config
   ```

Example

Return the system to the factory defaults:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#sys system-default
```

```
WARNING: Executing this command returns the system to factory defaults and deletes all
local configured user accounts.
This command needs system reset to take into effect
Do you want to continue (y/n) ? y
```

```
Switch:1#reset
```

The device reboots and the Admin user logs into the system again.

```
Switch:1(config)#save config
```

Configuring the password complexity rule

About this task

Use the following procedure to configure the password complexity rule.

The password complexity rule default is to use at least two uppercase, two lowercase, two numeric, and two special character to meet the password criteria.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the password complexity rule:

   ```
   password password-rule <1-2> <1-2> <1-2> <1-2>
   ```

3. **(Optional)** Configure the password complexity rule to the default:

   ```
   default password password-rule
   ```

4. Save the configuration:

   ```
   save config
   ```

   > ✴ **Note:**
   >
   > The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the password complexity rule to require two uppercase, two lowercase, two numeric and two special characters in each password:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password password-rule 2 2 2 2
Switch:1(config)#save config
```

Variable definitions

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

Variable	Value
<1–2> <1–2> <1–2> <1–2>	Configures the minimum password rule. The first variable defines the number of uppercase characters required. The second <1-2> variable defines the number of lowercase characters required. The third <1-2> variable defines the number of numeric characters required. The fourth <1-2> variable defines the number of special characters required. The default for each of these is 2.

Configuring the password length rule

About this task

Configure the password length rule after you enable enhanced secure mode. By default, the minimum password length is 15.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the password length rule option:

   ```
   password min-passwd-len <8-32>
   ```

3. **(Optional)** Configure the password length rule to the default:

   ```
   default password min-passwd-len
   ```

4. Save the configuration:

   ```
   save config
   ```

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

Example

Configure the password length rule to 20:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password min-passwd-len 20
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password min-passwd-len` command.

Variable	Value
<8–32>	Configures the minimum character length required. The default is 15.

Configuring the change interval rule

About this task

Use the following procedure to configure the change interval rule. The system enforces a minimum password change interval, which defines the minimum amount of time before you can change to a new password. By default, the minimum change interval is 24 hours between changing from one password to a new password.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the change interval rule option:

   ```
   password change-interval <1-999 hours>
   ```

3. **(Optional)** Configures the change interval rule to the default:

   ```
   default password change-interval
   ```

4. Save the configuration:

   ```
   save config
   ```

   > ⊛ **Note:**
   >
   > The **save config** command saves the configuration file with the filename configured as the primary configuration filename in **boot config**. Use the command **show boot config choice** to view the current primary and backup configuration filenames.

Example

Configure the change interval rule to 72 hours:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password change-interval 72
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password change-interval** command.

Variable	Value
<1–999>	Configures the minimum interval between consecutive password changes. The default is 24 hours.

Configuring the reuse rule

Use the following procedure to configure the password reuse rule. The default password reuse rule is 3.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

    enable

    configure terminal

2. Configure the password reuse rule option:

    password password-history *<3–32>*

3. **(Optional)** Configure the password reuse rule to the default:

    default password password-history

4. Save the configuration:

    save config

    ⁕ **Note:**

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

Example

Configure the reuse rule to 30:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password password-history 30
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **password password-history** command.

Variable	Value
<3–32>	Configures the minimum number of previous passwords to remember. The default is 3.

Configuring the maximum number of sessions

Use the following procedure to configure the maximum number of sessions on the switch. The max-sessions value configures the number of times a particular role-based user can log in to the switch through the SSH session at the same time. The default max-sessions value is 3.

The max-sessions value applies only for SSH sessions, and only with enhanced secure mode enabled.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the maximum number of sessions:

   ```
   password max-sessions <1–8> user-name WORD<1–255>
   ```

3. **(Optional)** Configure the password reuse rule to the default:

   ```
   default password max-sessions
   ```

4. Save the configuration:

   ```
   save config
   ```

   ⊛ **Note:**

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

Example

Configure the reuse rule to 5:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password max-sessions 5 user-name jsmith
Switch:1(config)#save config
```

Variable definitions

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

Variable	Value
<1–8>	Specifies the maximum number of sessions. The default is 3.
user-name *WORD<1–255>*	Specifies the user-name.

Configuring the maximum age rule

Use the following procedure to configure the maximum age rule.

If enhanced secure mode is enabled, the individual with the administrator access level role can configure the aging-time for each user. If you configure the aging time for each user, the aging time must be more than the global change interval value. The default is 90 days.

If you do not enable enhanced secure mode, the aging time is a global value for all users.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the maximum age rule option:

   ```
   password aging-time day <1–365> [user WORD<1–255>]
   ```

3. **(Optional)** Configure the maximum age rule to the default:

   ```
   default password aging-time [user WORD<1–255>]
   ```

4. Save the configuration:

   ```
   save config
   ```

   > ⊛ **Note:**
   >
   > The `save config` command saves the configuration file with the filename configured as the primary configuration filename in `boot config`. Use the command `show boot config choice` to view the current primary and backup configuration filenames.

Example

Configure the maximum age rule option to 100 days for user jsmith:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#password aging-time day 100 user jsmith
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the `password aging-time` command.

Variable	Value
day <1–365>	Configures the password aging time in days. The default is 90 days.

Table continues…

Variable	Value
user *WORD<1–255>*	Specifies a particular user.

Configuring the pre- and post-notification rule

Use the following procedure to configure the pre-notification and post-notification rule.

After enhanced secure mode is enabled, the switch enforces password expiry. To ensure a user does not lose access, the switch offers pre- and post-notification messages explaining when the password will expire.

The administrator can define pre- and post-notification intervals to between one to 99 days.

Before you begin

- You must enable enhanced secure mode in either the JITC or non-JITC sub-modes. It is recommended that you use the non-JITC sub-mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

About this task

The pre-notification intervals provide messages to warn users that their passwords will expire within a particular timeframe:

- interval 1—By default, interval 1 is 30 days.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 1 day.

The post-notification intervals provide notification to users that their passwords have expired within a particular timeframe:

- interval 1—By default, interval 1 is 1 day.
- interval 2—By default, interval 2 is 7 days.
- interval 3—By default, interval 3 is 30 days.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure the pre-notification rule option:

   ```
   password pre-expiry-notification-interval <1-99> <1-99> <1-99>
   ```

3. Configure post-notification rule option:

   ```
   password post-expiry-notification-interval <1-99> <1-99> <1-99>
   ```

4. Configure the pre-notification rule to the default:

   ```
   default password pre-expiry-notification-interval
   ```

5. Configure the post-notification rule to the default:

   ```
   default password post-expiry-notification-interval
   ```

6. Save the configuration:

```
save config
```

⚹ **Note:**

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

Example

Configure the pre- and post-notification rules to the default:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#default password pre-expiry-notification-interval
Switch:1(config)#default password post-expiry-notification-interval
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **pre-expiry-notification-interval** command.

Variable	Value
<1–99> <1–99> <1–99>	Configure the pre-notification intervals to provide messages to warn the users that their passwords will expire within a particular timeframe.
	The first <1–99> variable specifies the first notification, the second <1–99> specifies the second notification, and the third <1–99> variable specifies the third interval.
	By default, the first interval is 30 days, the second interval is 7 days, and the third interval is 1 day.

Use the data in the following table to use the **post-expiry-notification-interval** command.

Variable	Value
<1–99> <1–99> <1–99>	Configure the post-notification intervals to provide notification to the users that their passwords have expired within a particular timeframe.
	The first <1–99> variable specifies the first notification, the second <1–99> specifies the second notification, and the third <1–99> variable specifies the third interval.
	By default, the first interval is 1 day, the second interval is 7 days, and the third interval is 30 days.

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 pane, expand the **Configuration** > **Security** > **Control Path** folders.

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.
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.

Table continues…

Name	Description
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.

Changing passwords

About this task

Configure new passwords for each access level, or change the logon or password for the different access levels of the system to prevent unauthorized access. After you receive the switch, use default passwords to initially access CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change passwords in encrypted format.

Procedure

1. In the navigation pane, expand the **Configuration** > **Security** > **Control Path** folders.
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.

Table continues…

System access

Name	Description
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 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.

On IPv6 networks, the switch supports SSH server, remote login (rlogin) server and Remote Shell (rsh) server only. The switch does not support outbound SSH client over IPv6, rlogin client over IPv6 or rsh client over IPv6. On IPv4 networks, the switch 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 pane, expand the **Configuration** > **Security** > **Control Path** folders.

2. Click **Access Policies**.

3. Click the **Access Policies** tab.

4. Click **Insert**.

5. In the **ID** field, type the policy ID.

6. In the **Name** field, type the policy name.

7. Select the **PolicyEnable** check box.

8. Select the **Mode** option to allow or deny a service.

   If you configure the access policy mode to **deny**, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to **deny**, the system does not check **AccessLevel** and **AccessStrict** information. If you configure the access policy mode to allow, the system continues to check the **AccessLevel** and **AccessStrict** information.

9. From the **Service** options, select a service.

10. In the **Precedence** field, type a precedence number for the service (lower numbers mean higher precedence).

11. Select the **NetInetAddrType**.

12. In the **NetInetAddress** field, type an IP address.

13. In the **NetInetAddrPrefixLen** field, type the prefix length.

14. In the **TrustedHostInet Address** field, type an IP address for the trusted host.

15. In the **TrustedHostUserName** field, 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** check box, 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. If you configure the access policy mode to **deny**, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to **deny**, the system does not check **AccessLevel** and **AccessStrict** information. If you configure the access policy mode to allow, the system continues to check the **AccessLevel** and **AccessStrict** information.
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. Express IPv6 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.You do not need to provide this information if you select the NetInetAddrType of any. If the type is IPv6, you must enter an IPv6 address. You do not need to provide this information if you select the NetInetAddrType of any.
NetInetAddrPrefixLen	Indicates the source network Inet address prefix-length/mask. If the type is IPv4, you must enter an IPv4 address and mask length. 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.

Table continues…

Name	Description
	ⓘ 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. 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 (cleared).

Enabling an access policy

About this task

Enable the access policy feature globally to control access across the switch.

You can create an access policy to control access to the switch. An access policy specifies the hosts or networks that can access the switch through access services; for example Telnet, SNMP, Hypertext Transfer Protocol (HTTP), and remote login (rlogin).

Procedure

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

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **System Flags** tab.

5. Select the **EnableAccessPolicy** check box.

6. Click **Apply**.

System access security enhancements using EDM

The section provides information to enable enhanced secure mode.

Enabling enhanced secure mode

Use the following procedure to enable enhanced secure mode in either the JITC or non-JITC sub-modes.

The enhanced secure mode is disabled by default.

About this task

After you enable enhanced secure mode, the system can provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.

After you disable enhanced secure mode, the authentication, access-level, and password requirements work similarly to any of the existing commercial releases.

✴ Note:

You can use EDM to enable or disable enhanced secure mode. To configure the security enhancements this feature provides, you must use CLI.

Procedure

1. On the Device Physical View, select the device.

2. In the navigation pane, expand the **Configuration** > **Edit** folders.

3. Click **Chassis**.

4. Click the **Boot Config** tab.

5. In the **EnableEnhancedsecureMode** option box, select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. Select **disable** to disable the enhanced secure mode.

   ⊛ **Note:**

   It is recommended that you enable the non-JITC sub-mode. The JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.

6. Click **Apply**.

7. Save the configuration, and restart the switch.

Chapter 17: CLI show command reference

The following reference information provides show commands to view the operational status of the switch.

Access, logon names, and passwords

Use the **show cli password** command to display the access, logon name, and password combinations. The syntax for this command is as follows.

show cli password

The following example shows output from the **show cli password** command if enhanced secure mode is disabled.

```
Switch:1#show cli password
        access-level
        aging      90

        min-passwd-len 10
        password-history 3

        ACCESS     LOGIN          STATE
        rwa        rwa            NA
        rw         rw             ena
        l3         l3             ena
        l2         l2             ena
        l1         l1             ena
        ro         ro             ena
        Default Lockout Time      60
        Lockout-Time:
                   IP             Time
```

The following example shows output from the **show cli password** command if enhanced secure mode is enabled.

⊛ **Note:**

After you enable enhanced secure mode, the parameters in the output for the **show cli password** command apply to all of the role-based users, except for the admin user. So for instance, the system mandates that the admin user must have a password length of 15, and a password with two of each of the following characters: uppercase, lowercase, numeric and special character. However, the admin user can then configure this differently for the other user access levels. The following values that display for min-passwd-len and password-rule are

those configured by admin, and they apply to the privilege, operator, security, and auditor access levels.

```
Switch:1#show cli password
        change-interval 24
        min-passwd-len 8
        password-history 3
        password-rule 1 1 1 1
        pre-expiry-notification-interval 1 7 30
        post-expiry-notification-interval 1 7 30
        access-level
        ACCESS          LOGIN       AGING  MAX-SSH-SESSIONS  STATE
        admin           rwa         90     3                 ena
        privilege                   90     3                 dis
        operator        oper1       90     3                 ena
        security        security    90     3                 ena
        auditor         auditor     90     3                 ena
        Default Lockout Time        60
        Lockout-Time:
```

Basic switch configuration

Use the **show basic config** command to display the basic switch configuration. The syntax for this command is as follows.

show basic config

The following example shows the output of this command.

```
Switch:1#show basic config
                     setdate : N/A
                     auto-recover-delay : 30
```

Current switch configuration

Use the **show running-config** command to display the current switch configuration. The syntax for this command is as follows.

show running-config [verbose] [module <boot|cfm|cli|diag|dvr|fa|fhs| filter|ip|ipv6|isis|i-sid|lacp|lldp|macsec|mlt|naap|nsna|ntp|port|qos| radius|rmon|sflow|slamon|slpp|smtp|spbm|stg|sys|tacacs|vlan|web|vxlan>]

✱ **Note:**

All configuration modules are not supported on all hardware platforms. For more information about feature support, see *Release Notes*.

The following table explains parameters for this command.

Table 16: Command parameters

Parameter	Description
module <boot|cfm|cli|diag|dvr|fa|fhs|filter|ip|ipv6|isis|i-sid|lacp|lldp|macsec|mlt|naap|nsna|ntp|port|qos|radius|rmon|sflow|slamon|slpp|smtp|spbm|stg|sys|tacacs|vlan|web|vxlan>	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.

```
Switch:1#show running-config
Preparing to Display Configuration...
#
# Sun Jan 04 14:04:23 1970 UTC
# box type              : VSP-8284XSQ
# software version      : vsp8k_4.0_B017 (PRIVATE)
# cli mode              : CLI    #

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

⊛ **Note:**

> The output from the **show running-config** command displays an "end statement" near the end of the config file. This statement means that the script is exiting the Global Configuration mode and loading the rest of the configuration in Privileged EXEC mode, which is a requirement when loading the IP redistribution commands.

If you add **verbose** to the **show running-config** command, the output contains current switch configuration including software (versions), performance, VLANs (numbers, port members), ports (type, status), routes, memory, interface, and log and trace files. With the verbose command, you can view the current configuration and default values.

CLI settings

Use the **show cli info** command to display information about the CLI configuration. The syntax for this command is as follows.

show cli info

The following example shows sample output from the **show cli info** command.

```
Switch:1#show cli info

cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
```

Administering VOSS

```
timeout          : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt     : true
default login prompt         : Login:
custom login prompt          : Login:
use default password prompt : true
default password prompt      : Password:
custom password prompt       : Password:
prompt : Switch
```

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.

```
Switch:1#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.

You can identify a port licensed VSP 7200 Series switch with its part number. Use the command `show sys-info` to view the part number of the switch. For the list of part numbers of VSP 7200 Series switches with the option of port licensing, see *Installing the Avaya Virtual Services Platform 7200 Series*, NN47228-302.

The syntax for this command is as follows:

show sys-info [card] [fan] [led] [power] [temperature] [uboot]

The following table explains the parameters for this command.

Table 17: Command parameters

Parameter	Description
card	Displays information about the device. Includes type, serial number and assembly date.

Table continues…

Parameter	Description
	✱ **Note:** Not all hardware platforms support removable cards or modules. If a platform does not support cards, the output provides information on the chassis as a whole. For more information, see the hardware documentation for your platform.
fan	Displays information about installed cooling ports.
led	Displays LED information in detail.
power	Displays information about installed power supplies.
temperature	Displays temperature information.
uboot	Displays uboot details.

The following example shows partial output from the **show sys-info** command for VSP 8284XSQ. The output for this command can be different for other VOSS switches because of hardware differences.

```
Switch:1>show sys-info

General Info :

        SysDescr      : VSP-8284XSQ (4.2.1.0) (DEV)
        SysName       : Switch
        SysUpTime     : 0 day(s), 15:49:09
        SysContact    : http://support.avaya.com/
        SysLocation   : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis            : 8284XSQ
        ModelName          : 8284XSQ
        BrandName          : Avaya
        Serial#            : SDNIV84Q2002
        H/W Revision       : 1
        H/W Config         :
        NumSlots           : 2
        NumPorts           : 85
        BaseMacAddr        : b0:ad:aa:41:34:00
        MacAddrCapacity    : 1024
        MgmtMacAddr        : b0:ad:aa:41:34:81
        System MTU         : 1950

Card Info :

        Slot#      CardType        Serial#            Part#    Oper    Admin   Power
                                                               Status  Status  State

            1      8242XSQ     SDNIV84Q2002              --      up      up      on

            2      8242XSQ     SDNIV84Q2002              --      up      up      on


Temperature Info :

```

```
    CPU Temperature    MAC Temperature   PHY1 Temperature   PHY2 Temperature

              31                 35                 27                 30



Power Supply Info :


        Ps#1 Status        : up
        Ps#1 Type          : AC
        Ps#1 Description   : DPS-800RB D
        Ps#1 Serial Number: GWXD1415000060
        Ps#1 Version       : S1F
        Ps#1 Part Number   : 700508298
        Ps#2 Status        : empty

        Total Power Available : 800 watts

Fan Info :


        Fan#1 Status           : up
        Fan#1 Type             : regularSpeed
        Fan#1 FlowType         : front-back

        Fan#2 Status           : up
        Fan#2 Type             : regularSpeed
        Fan#2 FlowType         : front-back
LED Info :


        LED#1 Label  : PWR
        LED#1 Status : GreenSteady


        LED#2 Label  : Status
        LED#2 Status : GreenSteady


        LED#3 Label  : Rps
        LED#3 Status : Off


        LED#4 Label  : Fan
        LED#4 Status : GreenSteady


System Error Info :


        Send Login Success Trap  : false
        Send Authentication Trap  : false
        Error Code               : 0
        Error Severity           : 0


Port Lock Info :


        Status      : off
        LockedPorts :
```

```
Message Control Info :


        Action               : suppress-msg
        Control-Interval     : 30
        Max-msg-num          : 5
        Status               : enable




Configuration Operation Info :

         Last Change: 0 day(s), 10:37:22
    Last Vlan Change: 0 day(s), 06:42:58
Last Statistic Reset: 0 day(s), 00:00:00
```

The following example shows the partial output of the **show sys-info** command on a VSP 7254XSQ switch. The part number EC720003X-E6 indicates it is a port licensed switch.

```
Switch:1#show sys-info

General Info :

        SysDescr     : VSP-7254XSQ (5.1.0.0_B682) (PRIVATE)
        SysName      : SF-237:1
        SysUpTime    : 9 day(s), 00:30:59
        SysContact   : http://support.avaya.com/
        SysLocation  : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis             : 7254XSQ
        Serial#             : 15JP113CF01L
        H/W Revision        : 00
        H/W Config          :
        Part Number         : EC720003X-E6
        NumSlots            : 2
        NumPorts            : 73
        BaseMacAddr         : a4:25:1b:54:9c:00
        MacAddrCapacity     : 1024
        MgmtMacAddr         : a4:25:1b:54:9c:81
        System MTU          : 1950
```

Use the **show interfaces gigabtethernet** command to display the port information of the switch.

On a VSP 7200 Series switch that is port licensed, use the command **show interfaces gigabitethernet** to view the licensed status of the ports on the switch.

The syntax for this command is as follows:

show interfaces gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}

The following example shows output for the **show interfaces gigabitethernet 1/41 – 1/42** command. Slot and port information can differ depending on hardware platform. For more information, see your hardware documentation.

```
Switch:1#show interfaces gigabitEthernet 1/41-1/42
================================================================================
                                                Port

Interface
```

```
======================================================================
PORT                                            LINK    PORT
PHYSICAL                    STATUS
NUM      INDEX     DESCRIPTION      TRAP    LOCK    MTU     ADDRESS
ADMIN        OPERATE
----------------------------------------------------------------------
1/41  232   40GbNone       true   false   1950  b0:ad:aa:41:34:28 down   down
1/42  233   40GbNone       true   false   1950  b0:ad:aa:41:34:29 down   down
```

The following example shows the partial output of the **show interfaces gigabitethernet** command for the VSP 7254XSQ switch. View the LICENSE STATUS field. It can have one of the following values:

- n/a: Indicates that it is not a port that is activated by a port license.

- locked: Indicates that the port is locked and non-operational because the switch is port licensed and a valid port license is not present.

  Attempting to enable a locked port, for example port 1/25, displays the error message Error: port 1/25, Port License is required to enable this port.

- unlocked: Indicates that the port is unlocked and is operational, because a valid port license is present.

```
Switch:1#show interfaces gigabitEthernet

===============================================================================
                                  Port Interface
===============================================================================
PORT                      LINK  PORT          PHYSICAL          STATUS        LICENSE
NUM      INDEX DESCRIPTION TRAP  LOCK    MTU   ADDRESS           ADMIN OPERATE STATUS
-------------------------------------------------------------------------------
1/1    192   10GbNone      true  false   1950  a4:25:1b:54:9c:00 up    down    n/a
1/2    193   10GbNone      true  false   1950  a4:25:1b:54:9c:01 down  down    n/a
1/3    194   10GbNone      true  false   1950  a4:25:1b:54:9c:02 down  down    n/a
1/4    195   10GbNone      true  false   1950  a4:25:1b:54:9c:03 down  down    n/a
1/5    196   10GbNone      true  false   1950  a4:25:1b:54:9c:04 down  down    n/a
1/6    197   10GbNone      true  false   1950  a4:25:1b:54:9c:05 down  down    n/a
1/7    198   10GbNone      true  false   1950  a4:25:1b:54:9c:06 down  down    n/a
1/8    199   10GbNone      true  false   1950  a4:25:1b:54:9c:07 down  down    n/a
1/9    200   10GbNone      true  false   1950  a4:25:1b:54:9c:08 down  down    n/a
1/10   201   10GbNone      true  false   1950  a4:25:1b:54:9c:09 down  down    n/a
1/11   202   10GbNone      true  true    1950  a4:25:1b:54:9c:0a up    down    n/a
1/12   203   10GbNone      true  false   1950  a4:25:1b:54:9c:0b down  down    n/a
1/13   204   10GbNone      true  false   1950  a4:25:1b:54:9c:0c down  down    n/a
1/14   205   10GbNone      true  false   1950  a4:25:1b:54:9c:0d up    down    n/a
1/15   206   10GbNone      true  false   1950  a4:25:1b:54:9c:0e up    down    n/a
1/16   207   10GbCX        true  false   1950  a4:25:1b:54:9c:0f up    up      n/a
1/17   208   10GbNone      true  false   1950  a4:25:1b:54:9c:10 down  down    n/a
1/18   209   10GbNone      true  false   1950  a4:25:1b:54:9c:11 down  down    n/a
1/19   210   10GbNone      true  false   1950  a4:25:1b:54:9c:12 down  down    n/a
1/20   211   10GbNone      true  false   1950  a4:25:1b:54:9c:13 down  down    n/a
1/21   212   10GbNone      true  false   1950  a4:25:1b:54:9c:14 up    down    n/a
1/22   213   10GbNone      true  false   1950  a4:25:1b:54:9c:15 up    down    n/a
1/23   214   10GbNone      true  false   1950  a4:25:1b:54:9c:16 down  down    n/a
1/24   215   10GbNone      true  false   1950  a4:25:1b:54:9c:17 up    down    n/a
1/25   216   10GbNone      true  false   1950  a4:25:1b:54:9c:18 down  down    unlocked
1/26   217   10GbNone      true  false   1950  a4:25:1b:54:9c:19 down  down    unlocked
1/27   218   10GbNone      true  false   1950  a4:25:1b:54:9c:1a down  down    unlocked
1/28   219   10GbNone      true  false   1950  a4:25:1b:54:9c:1b down  down    unlocked
1/29   220   10GbNone      true  false   1950  a4:25:1b:54:9c:1c down  down    unlocked
1/30   221   10GbNone      true  false   1950  a4:25:1b:54:9c:1d down  down    unlocked
1/31   222   10GbNone      true  false   1950  a4:25:1b:54:9c:1e down  down    unlocked
1/32   223   10GbNone      true  false   1950  a4:25:1b:54:9c:1f down  down    unlocked
1/33   224   10GbNone      true  false   1950  a4:25:1b:54:9c:20 down  down    unlocked
1/34   225   10GbNone      true  false   1950  a4:25:1b:54:9c:21 down  down    unlocked
1/35   226   10GbNone      true  false   1950  a4:25:1b:54:9c:22 down  down    unlocked
1/36   227   10GbNone      true  false   1950  a4:25:1b:54:9c:23 down  down    unlocked
1/37   228   10GbNone      true  false   1950  a4:25:1b:54:9c:24 down  down    unlocked
1/38   229   10GbNone      true  false   1950  a4:25:1b:54:9c:25 down  down    unlocked
1/39   230   10GbNone      true  false   1950  a4:25:1b:54:9c:26 down  down    unlocked
```

```
1/40     231   10GbNone          true   false   1950  a4:25:1b:54:9c:27 down   down   unlocked
1/41     232   10GbNone          true   false   1950  a4:25:1b:54:9c:28 down   down   unlocked
1/42     233   10GbNone          true   false   1950  a4:25:1b:54:9c:29 down   down   unlocked
1/43     234   10GbNone          true   false   1950  a4:25:1b:54:9c:2a down   down   unlocked
1/44     235   10GbNone          true   false   1950  a4:25:1b:54:9c:2b down   down   unlocked
1/45     236   10GbNone          true   false   1950  a4:25:1b:54:9c:2c down   down   unlocked
1/46     237   10GbNone          true   false   1950  a4:25:1b:54:9c:2d down   down   unlocked
1/47     238   10GbNone          true   false   1950  a4:25:1b:54:9c:2e down   down   unlocked
1/48     239   10GbNone          true   false   1950  a4:25:1b:54:9c:2f down   down   unlocked
2/1      256   40GbNone          true   false   1950  a4:25:1b:54:9c:40 up     down   n/a
2/2      260   40GbNone          true   false   1950  a4:25:1b:54:9c:44 down   down   n/a
2/3      264   40GbNone          true   false   1950  a4:25:1b:54:9c:48 down   down   n/a
2/4      268   40GbNone          true   false   1950  a4:25:1b:54:9c:4c down   down   n/a
2/5/1    272   40GbNone-Channel true   false   1950  a4:25:1b:54:9c:50 down   down   unlocked
2/5/2    273   40GbNone-Channel true   false   1950  a4:25:1b:54:9c:51 down   down   unlocked
2/5/3    274   40GbNone-Channel true   false   1950  a4:25:1b:54:9c:52 down   down   unlocked
2/5/4    275   40GbNone-Channel true   false   1950  a4:25:1b:54:9c:53 down   down   unlocked
2/6      276   40GbNone          true   false   1950  a4:25:1b:54:9c:54 down   down   unlocked
```

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.

```
Switch:1##show ntp statistics
  N     NTP Server : 192.0.2.187
----------------------------------------
              Stratum : unknown
              Version : unknown
          Sync Status : unknown
         Reachability : unknown
           Root Delay : unknown
            Precision : unknown
      Access Attempts : 0
         Server Synch : 0
          Server Fail : 0
          Fail Reason : unknown
```

Power summary

Use the `show sys power` command to view a summary of the power information for the chassis.

The syntax for this command is as follows.

`show sys power [global] [power-supply] [slot]`

The following example shows sample command output.

```
Switch:1#show sys power

================================================================================
                          Chassis Power Information
================================================================================

Chassis Power Status: non-redundant

            Total       Required  Max
Chassis     Chassis     Redundant Allocated Available
Type        Power       Power     Power     Power
--------------------------------------------------------------------------------
SwitchXYZ     800          0        145       655
--------------------------------------------------------------------------------
```

⊛ **Note:**

Power information can differ by hardware platform. For more information, see the hardware documentation for your platform.

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.

```
Switch:1#show sys power power-supply

================================================================================
                          Power Supply Information
================================================================================
Power    Type   Input   Serial           Part           Oper   Max
Supply          Voltage Num              Num            Status Power
--------------------------------------------------------------------------------
PS#2     AC     110/220 GWXD1349000116-  DPS-800RB        up     800
--------------------------------------------------------------------------------
```

⊛ **Note:**

Power information can differ depending on hardware platform. For more information, see the hardware documentation for your platform.

System information

Use the `show sys` command to display system status and technical information about the switch hardware components and software configuration. The command shows several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information. The syntax for this command is as follows.

```
show sys <dns|force-msg|mgid-usage|msg-control|mtu|power|setting|
software|stats|topology-ip>
```

The following table explains parameters for this command.

Table 18: Command parameters

Parameter	Description
dns	Shows the DNS default domain name.
force-msg	Shows the message control force message pattern settings.
mgid-usage	Shows the multicast group ID (MGID) usage for VLANs and multicast traffic.
msg-control	Shows the system message control function status (activated or disabled).
mtu	Shows system maximum transmission unit (MTU) information.
power	Shows power information for the chassis. Command options are • 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 *Monitoring Performance*.
topology-ip	Shows the circuitless IP set.

The following example shows output from the `show sys dns` command.

```
Switch:1>show sys dns
        DNS Default Domain Name :
        Primary DNS server details:
        ===========================
                IP address : 10.1.1.1
                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.

```
Switch:1#show sys mgid-usag
        Number of MGIDs used for VLANs : (6)
        Number of MGIDs used for multicast : (0)
        Number of MGIDs used for SPBM : (0)
        Number of MGIDs remaining for VLANs : (4089)
        Number of MGIDs remaining for multicast : (6976)
        Number of MGIDs remaining for SPBM : (1024)
```

The following example shows output from the **show sys msg-control** command.

```
Switch: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.

```
Switch:1#show sys setting
                udp-checksum : enable
           mroute-stream-limit : disable
                     contact : http://company.com/
                    location : Anywhere, USA
                        name : Switch
                    portlock : off
        sendAuthenticationTrap : false
                autotopology : on
           ForceTopologyIpFlag : false
            clipId-topology-ip : 0
                         mtu : 1950
     data-path-fault-shutdown : enable
```

The following example shows output from the **show sys software** command.

```
Switch:1#show sys software

System Software Info :

Default Runtime Config File : /intflash/config.cfg
Config File :
Last Runtime Config Save : 0

Boot Config Table
Version : Build 4.1.0.0 (GA) on Fri May 30 18:04:13 EDT 2014
PrimaryConfigSource : /intflash/config.cfg
SecondaryConfigSource : /intflash/config.cfg
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : false
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : false
```

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 ports), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), Virtual Router Redundancy Protocol (VRRP), 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.

```
Switch:1#show tech

Sys Info:
---------------


General Info :

        SysDescr      : VSP-8284XSQ (4.0.0.0)
        SysName       : VSP-8284XSQ
        SysUpTime     : 3 day(s), 14:22:52
        SysContact    : http://support.avaya.com/
        SysLocation   : 211 Mt. Airy Road,Basking Ridge,NJ 07920

Chassis Info:

        Chassis           : 8284XSQ
        ModelName         : 8284XSQ
        BrandName         : Avaya
        Serial#           : 12JP442H70YC
        H/W Revision      : 10
        H/W Config        : none
        NumSlots          : 1
        NumPorts          : 50
        BaseMacAddr       : 24:d9:21:e2:e0:00
        MacAddrCapacity   : 256

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

Telnet-access sessions

Use the **show telnet-access** command to display to show the total sessions allowed. The syntax for this command is as follows.

show telnet-access

The following example shows output from the **show telnet-access** command.

```
Switch:1#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.

```
Switch:1#show users
SESSION    USER                 ACCESS    IP ADDRESS
Telnet0    rwa                  rwa       192.0.2.24 (current)
Console                         none      ----------
```

Port egress COS queue statistics

Use the **show qos cosq-stats interface** command to retrieve the port egress COS queue statistics. The syntax for this command is as follows:

show qos cosq-stats interface {slot/port[/sub-port][-slot/port[/sub-port]][,...]}

The following example shows output from the **show qos cosq-stats interface** command.

```
Switch:1#show qos cosq-stats interface 1/42

================================================================================
                       Port:1/42  QOS CoS Queue Stats
================================================================================
CoS  Out Packets          Out Bytes          Drop Packets        Drop Bytes
--------------------------------------------------------------------------------
0    0                    0                  0                   0
1    0                    0                  0                   0
2    0                    0                  0                   0
3    0                    0                  0                   0
4    0                    0                  0                   0
5    0                    0                  0                   0
6    0                    0                  0                   0
7    0                    0                  0                   0
Switch:1#
```

CPU queue statistics

Use the **show qos cosq-stats cpu-port** command to display the statistics of the forwarded packets and bytes, and the dropped packets and bytes, for the traffic sent toward the CP. The

queue assignment is based on the protocol types, not on the internal COS value. These statistics are useful for debugging purposes.

The syntax for this command is as follows:

show qos cosq-stats cpu-port

The following example shows output from the **show qos cosq-stats cpu-port** command.

```
Switch:1#show qos cosq-stats cpu-port

================================================================================
                    QOS CoS Queue Cpu Port Stats Table
================================================================================
CoS   Out Packets         Out Bytes           Drop Packets        Drop Bytes
--------------------------------------------------------------------------------
0     0                   0                   0                   0
1     0                   0                   0                   0
2     0                   0                   0                   0
3     0                   0                   0                   0
4     0                   0                   0                   0
5     0                   0                   0                   0
6     414                 35714               0                   0
7     0                   0                   0                   0
8     561                 41738               0                   0
9     28740               1969460             0                   0
10    12005               2006662             0                   0
11    0                   0                   0                   0
12    0                   0                   0                   0
13    0                   0                   0                   0
14    7280                495040              0                   0
15    0                   0                   0                   0
```

Chapter 18: Port numbering and MAC address assignment reference

This section provides information about the port numbering and Media Access Control (MAC) address assignment used on the switch.

Port numbering

A port number includes the slot location of the port in the chassis, as well as the port position. For example, the first port in the first slot is structured as 1/1. The number of slots and ports varies depending on the hardware platform. For more information about hardware, see the hardware documentation for your platform.

VSP 4000

The following diagrams illustrate the components on the front panels of the Avaya VSP 4000 switches.

Figure 9: VSP 4850GTS

1. VSP 4000 USB cover
2. Switch LEDs
3. 10/100/1000 ports (LEDs above ports)
4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.
5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.
6. Console Port
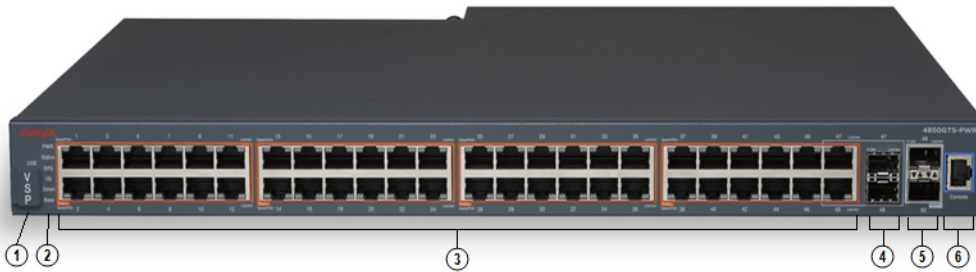
Figure 10: VSP 4850GTS-PWR+

1. VSP 4000 USB cover

2. Switch LEDs

3. 10/100/1000 PoE+ ports (LEDs above ports)

4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.

5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.
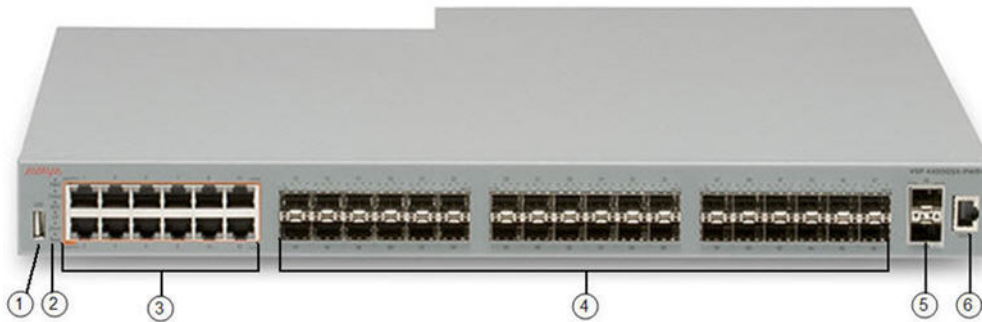
6. Console Port

Figure 11: VSP 4450GSX-PWR+

1. VSP 4000 USB port

2. Switch LEDs

3. 10/100/1000 Base TX RJ-45 ports with PoE+ (LEDs above ports)

4. 100/1000 Mbps SFP transciever modules

5. 1/10G SFP + ports

6. Console Port
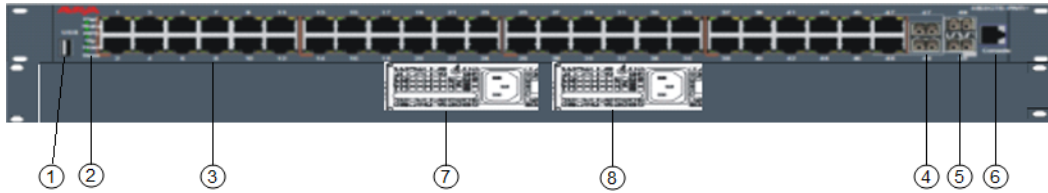
Figure 12: VSP 4450GTX-HT-PWR+

1. VSP 4000 USB port but without a USB or a USB device cover

⊛ **Note:**

The VSP 4450GTX-HT-PWR+ model does not require a USB device in the USB port for normal operation. The USB port can be used for additional storage using a USB memory stick.

2. Switch LEDs

3. 10/100/1000 Base TX RJ-45 ports with 802.3at PoE+

4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs

5. SFP+ slots. Supports Avaya 1G SFPs and 10G SFP+s

6. Console Port

7. Field-replaceable 1000W AC power supply unit (PSU)

8. Second field-replaceable AC power supply unit for redundancy or additional PoE

Figure 13: VSP 4450GSX-DC

1. VSP 4000 USB cover

2. Switch LEDs

3. 10/100/1000 ports (LEDs above ports)

4. Combo port SFP slots. Supports Avaya 1G SFPs and 100Base low speed SFPs.

5. SFP+ slots. Supports Avaya's 1G SFPs and 10G SFP+s.

6. Console Port

VSP 7200

The following figure illustrates the front view of the VSP 7200 switch.

When looking at the front of the switch:

- Slot 1 is the grouping of 48 ports.

Comments on this document? infodev@avaya.com

- Slot 2 is the grouping of 6 40 Gbps ports to the right.
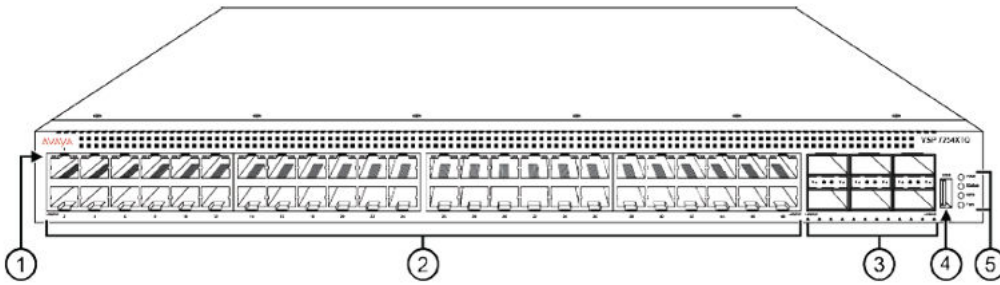
1. LEDs indicating port activity are above the RJ-45 and SFP+ port. The up arrow on the left indicates the top port; the down arrow on the right indicates the bottom port.

2. 48 ports — The VSP 7254XSQ has 48 SFP/SFP+ fiber ports. The VSP 7254XTQ has 48 RJ-45 copper ports.

3. Six QSFP+ ports — The LEDs are below each port. There are four LEDs per port to support channelization. The up arrows refer to the port above.

4. USB port

5. LEDs for system power (PWR), switch status (Status), redundant power supply (RPS), and fan modules (Fan).

VSP 8000

The following diagrams illustrate the components on the front panels of the switches. For more information on hardware, see *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.

The following figure illustrates the front view of the VSP 8200 switch. There are 40 ports in Slot 1 on top, and 40 ports in Slot 2 on the bottom.
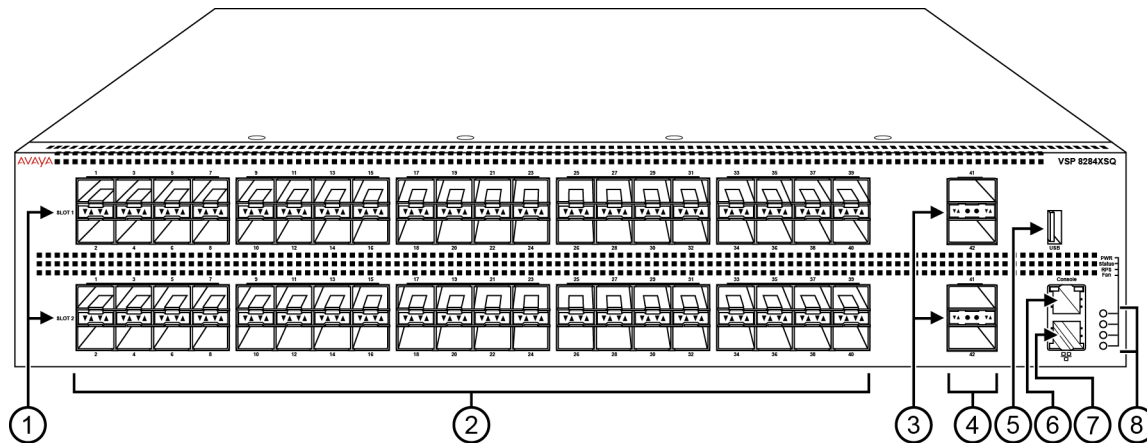
Figure 14: VSP 8284XSQ front view

1. SFP+ port LEDs are in between the ports on each slot. The up arrows refer to the port above and the down arrows refer to the port below.

Table continues…

2. 80 SFP+ ports that support Avaya's 1G SFPs and 10G SFP+s.

• 40 ports in Slot 1 on top

• 40 ports in Slot 2 on the bottom

3. QSFP+ port LEDs are in between the ports on each slot. The up arrows refer to the port above and the down arrows refer to the port below.

4. Four QSFP+ ports: two in Slot 1 and two in Slot 2.

5. USB port

6. Console port (10101)

7. Management port — The LEDs are on the bottom of the port.

8. LEDs for system power (PWR), switch status (Status), redundant power supply (RPS), and fan modules(Fan).

The following figure illustrates the front view of the VSP 8400 switch.
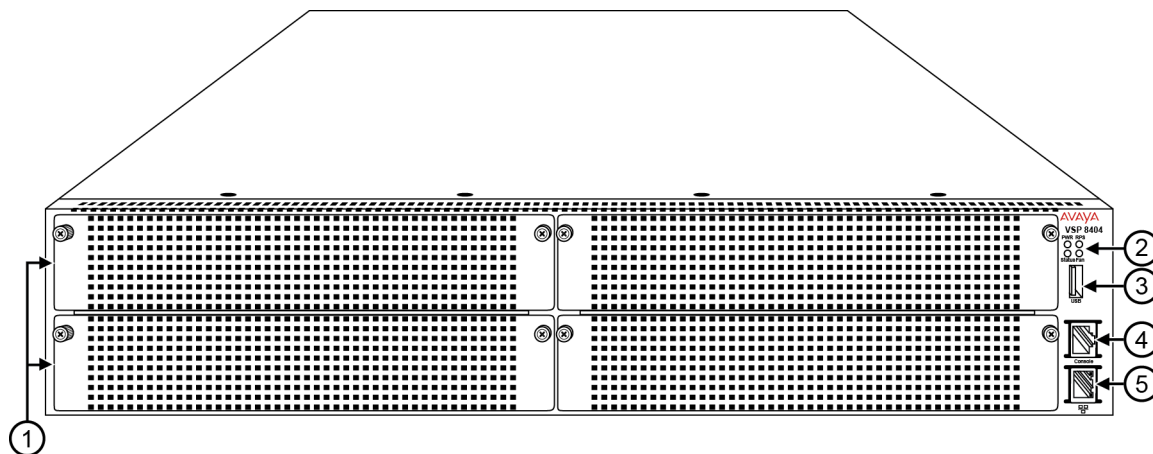
Figure 15: VSP 8404 front view

Looking at the front of the switch, slot numbering begins at the top row and increases from left to right. Slot 1 is the top-left slot; slot 2 is the top-right slot. Slot 3 is the bottom-left slot; slot 4 is the bottom-right slot.

Port numbering depends on the type of Ethernet Switch Module (ESM) installed in the slot. For more information about ESMs, see *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.

1. Displays the four slots to install ESMs.

2. LEDs for system power (PWR), switch status (Status), redundant power supply (RPS), and fan modules (Fan).

3. USB port

4. Console port

5. OOB management port

Interface indexes

The Simple Network Management Protocol (SNMP) uses interface indexes to identify ports, Virtual Local Area Networks (VLAN), and Multilink Trunking (MLT).

Port interface index

To determine the interface index (IfIndex), you can calculate it, or use the CLI command provided in this section.

As a result of channelization support, the ifIndex of each channelization–capable port increases by 4. The number is reserved for the 3 sub-ports when channelization is enabled.

> ✱ **Note:**
>
> Slot and port information can vary depending on hardware platform. For more information, see the hardware documentation for your platform.
>
> Channelization is not supported by all platforms. For more information about feature support, see *Release Notes*.

VSP 4000 Series :

For switches that do not include channelization-capable ports, use the following equation to determine the IfIndex of a port:

```
(192 x slot number) + (port number – 1)
```

For example, the interface index of port 1/50 is 241.

The VSP 4000 Series uses one slot.

VSP 7200 Series and VSP 8000 Series:

For switches that include channelization-capable ports, use the following equations to determine the IfIndex of a port:

- If the port does not support channelization, use `(64 x slot number)  +128 + (port number -1)`.
- If the port supports channelization, use the following equations:
  - for the port in question: `(64 x slot number)  +128`
  - for subsequent ports: `(64 x slot number)  +128 +  ((port number  -1) *4)`

    This equation reserves space for the creation of the 3 sub-ports on the previous port, if or when you enable channelization.

The slot numbers are 1-2 for the VSP 7200 Series.

The slot numbers are 1-2 for the VSP 8200.

The slot numbers are 1-4 for VSP 8400.

CLI command:

To determine the port interface index through the CLI, use the following command:

```
show interfaces gigabitEthernet
```

The following example shows an output for this command:

```
Switch:1(config)#show interfaces gigabitEthernet

================================================================================
                                    Port Interface
================================================================================
PORT                       LINK  PORT          PHYSICAL                 STATUS
NUM    INDEX DESCRIPTION   TRAP  LOCK   MTU    ADDRESS           ADMIN  OPERATE
--------------------------------------------------------------------------------
1/1      192 10GbNone      true  false  1950   b0:ad:aa:41:90:00 up     down
1/2      193 10GbOther     true  false  1950   b0:ad:aa:41:90:01 up     down
1/3      194 10GbNone      true  false  1950   b0:ad:aa:41:90:02 up     down
1/4      195 10GbNone      true  false  1950   b0:ad:aa:41:90:03 up     down
1/5      196 10GbNone      true  false  1950   b0:ad:aa:41:90:04 up     down
1/6      197 10GbSR        true  false  1950   b0:ad:aa:41:90:05 up     down
1/7      198 10GbSR        true  false  1950   b0:ad:aa:41:90:06 up     down
1/8      199 GbicSx        true  false  1950   b0:ad:aa:41:90:07 up     down
1/9      200 10GbNone      true  false  1950   b0:ad:aa:41:90:08 up     down
1/10     201 10GbNone      true  false  1950   b0:ad:aa:41:90:09 up     down
1/11     202 10GbNone      true  false  1950   b0:ad:aa:41:90:0a up     down
1/12     203 10GbNone      true  false  1950   b0:ad:aa:41:90:0b up     down
1/13     204 10GbNone      true  false  1950   b0:ad:aa:41:90:0c up     down
1/14     205 10GbNone      true  false  1950   b0:ad:aa:41:90:0d up     down
1/15     206 10GbNone      true  false  1950   b0:ad:aa:41:90:0e up     down
1/16     207 GbicSx        true  false  1950   b0:ad:aa:41:90:0f up     down
1/17     208 40GbCR4       true  false  1950   b0:ad:aa:41:90:10 up     down
1/18/1   212 40GbSR4-Channel true false 1950   b0:ad:aa:41:90:14 up     up
1/18/2   213 40GbSR4-Channel true false 1950   b0:ad:aa:41:90:15 up     up
1/18/3   214 40GbSR4-Channel true false 1950   b0:ad:aa:41:90:16 up     up
1/18/4   215 40GbSR4-Channel true false 1950   b0:ad:aa:41:90:17 up     up
```

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 is assigned a base number of MAC addresses with a number reserved for ports and other internal purposes, and the remainder assigned to routable VLANs. The following table identifies the numbers provided by product.

Product	Base assignment	Reserved	Assigned to routable VLANs
VSP 4000 Series	256	First 128	remaining 128
VSP 7200 Series and VSP 8000 Series	1,024	First 256	256 and above

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 19: Supported standards, RFCs, and MIBs

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that the switch supports.

Supported IEEE standards

The following table details the IEEE standards that the switch supports.

✳ **Note:**

Feature support can vary by hardware platform. For more information about feature support, see *Release Notes*.

Table 19: Supported IEEE standards

IEEE standard	Description
802.1ag	Connectivity Fault Management
802.1ah	Provider Backbone Bridging
802.1aq	Shortest Path Bridging (SPB)
802.1AX	Link Aggregation
802.1D	MAC Bridges
P802.1p	Traffic Class Expediting & Dynamic Multicast Filtering
802.1Q	Virtual LANs
802.1s	Multiple Spanning Trees
802.1t	802.1D Technical & Editorial Corrections
802.1w	Rapid Spanning Tree Protocol (RSTP)
802.1X-2010	Port-based NAC
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Eletrotechnical Commission (IEC) 8802-3

Table continues…

IEEE standard	Description
802.3ab	1000 Mbps Operation, implemented as 1000BASE-T Copper
802.1AE	MAC Security
802.3ae	10 Gbps Operation, implemented as 10GBASE-X SFP+
802.3ba	40 Gbps and 100 Gbps Operation, implemented as 40GBASE-QSFP+
802.3x	Full Duplex & Flow Control
802.3z	1000 Mbps Operation, implemented as 1000BASE-X SFP

Supported RFCs

The following table and sections list the RFCs that the switch supports.

Table 20: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC 768	UDP Protocol
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet protocol
RFC 894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion control in IP/TCP internetworks
RFC 906	Bootstrap loading using TFTP
RFC 950	Internet Standard Subnetting Procedure
RFC 951	BootP
RFC 959, RFC 1350, and RFC 2428	FTP and TFTP client and server
RFC 1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC 1058	RIPv1 Protocol
RFC 1112	Host Extensions for IP Multicasting (IGMPv1)

Table continues…

Request for comment	Description
RFC 1122	Requirements for Internet Hosts
RFC 1253	OSPF MIB
RFC 1256	ICMP Router Discovery
RFC 1258	IPv6 Rlogin server
RFC 1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC 1340	Assigned Numbers
RFC 1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC 1541	Dynamic Host Configuration Protocol
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 1587	The OSPF NSSA Option
RFC 1591	DNS Client
RFC 1723	RIP v2 — Carrying Additional Information
RFC 1812	Router requirements
RFC 1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC 1981	Path MTU discovery
RFC 2068	Hypertext Transfer Protocol
RFC 2080	RIP
RFC 2131	Dynamic Host Control Protocol (DHCP)
RFC 2138	RADIUS Authentication
RFC 2139	RADIUS Accounting
RFC 2178	OSPF MD5 cryptographic authentication / OSPFv2
RFC 2233	The Interfaces Group MIB using SMIv2
RFC 2236	IGMPv2 Snooping
RFC 2358	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2284	PPP Extensible Authentication Protocol
RFC 2328	OSPFv2
RFC 2338	VRRP: Virtual Redundancy Router Protocol
RFC 2362	PIM-SM
RFC 2407	IP Security Domain Interpretation of Internet Security Association and Key Management Protocol (ISAKMP)

Table continues…

Request for comment	Description
RFC 2408	Internet Security Associations and Key Management Protocol (ISAKMP)
RFC 2453	RIPv2 Protocol
RFC 2460	IPv6 base stack
RFC 2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 2464	Transmission of IPv6 packets over Ethernet networks
RFC 2545	Use of BGP-4 multi-protocol extensions for IPv6 inter-domain routing
RFC 2548	Microsoft vendor specific RADIUS attributes
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance Statements for SMI v2
RFC 2616	Hypertext Transfer Protocol 1.1
RFC 2710	Multicast Listener Discovery (MLD) for IPv6
RFC 2716	PPP EAP Transport Level Security (TLS) Authentication Protocol
RFC 2819	RMON
RFC 2865	RADIUS
RFC 2874	DNS Extensions for IPv6
RFC 2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC 3046	DHCP Option 82
RFC 3162	IPv6 RADIUS client
RFC 3246	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3315	IPv6 DHCP Relay
RFC 3376	IGMPv3
RFC 3411 and RFC 2418	SNMP over IPv6 networks
RFC 3417	Transport Mappings for SNMP
RFC 3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC 3569	An overview of Source-Specific Multicast (SSM)
RFC 3579	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 3587	IPv6 Global Unicast Address Format
RFC 3748	Extensible Authentication Protocol
RFC 3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP

Table continues…

Request for comment	Description
RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 3986	Uniform Resource Identifiers (URI)
RFC 4007	IPv6 Scoped Address Architecture
RFC 4213	IPv6 configured tunnel
RFC 4250–RFC 4256	SSH server and client support
RFC 4291	IPv6 Addressing Architecture
RFC 4301	Security Architecture for IPv6
RFC 4302	IP Authentication Header (AH)
RFC 4303	IP Encapsulated Security Payload (ESP)
RFC 4305	Cryptographic algorithm implementation requirements for ESP and AH
RFC 4308	Cryptographic suites for Internet Protocol Security (IPsec)
RFC 4443	ICMP for IPv6
RFC 4541	Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping
RFC 4552	OSPFv3 Authentication and confidentiality for OSPFv3
RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM)
RFC 4607	Source-Specific Multicast (SSM)
RFC 4835	Cryptographic algorithm implementation for ESP and AH
RFC 4861	IPv6 Neighbor discovery
RFC 4862	IPv6 stateless address autoconfiguration
RFC 5095	Deprecation of Type 0 Routing headers in IPv6
RFC 5187	OSPFv3 Graceful Restart (helper-mode only)
RFC 5321	Simple Mail Transfer Protocol
RFC 5340	OSPF for IPv6
RFC 5798	Virtual Router Redundancy Protocol version 3
RFC 6105	IPv6 Router Advertisement Guard
RFC 6329	IS-IS Extensions supporting Shortest Path Bridging
RFC 7348	Virtual Extensible LAN (VXLAN)
RFC 7610	DHCPv6 Shield

Quality of service

Table 21: Supported request for comments

Request for comment	Description
RFC2474 and RFC2475	DiffServ Support
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB

Network management

Table 22: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (Revision 2)
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2428	FTP Extensions for IPv6
RFC2541	DNS Security Operational Considerations
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2616	IPv6 HTTP server
RFC2819	Remote Network Monitoring Management Information Base

Table continues…

Request for comment	Description
RFC 3411	Architecture for describing SNMP Management Frameworks
RFC4292	IP Forwarding Table MIB

MIBs

Table 23: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657	BGP-4 MIB using SMIv2
RFC2021	RMON MIB using SMIv2
RFC2452	IPv6 MIB: TCP MIB
RFC2454	IPv6 MIB: UDP MIB
RFC2466	IPv6 MIB: ICMPv6 Group
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)

Table continues…

Request for comment	Description
RFC4292	IP Forwarding Table MIB
RFC4363	Bridges with Traffic MIB

Standard MIBs

The following table details the standard MIBs that the switch supports.

Table 24: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib

Table continues…

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934	rfc2934.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	

Table continues…

Administering VOSS

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control protocol (TCP)	RFC4022	rfc4022.mib
STDMIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
Q-BRIDGE-MIB —Management Information Base for managing Virtual Bridged LANs	RFC4363	rfc4363-q.mib

Proprietary MIBs

The following table details the proprietary MIBs that the switch supports.

Table 25: Proprietary MIBs

Proprietary MIB name	File name
Avaya IGMP MIB	rfc_igmp.mib
Avaya IP Multicast MIB	ipmroute_rcc.mib
Avaya MIB definitions	wf_com.mib
Avaya PIM MIB	pim-rcc.mib
Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Avaya SLA Monitor Agent MIB	slamon.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5emt103.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definition for Combo Ports	s5ifx.mib
Other SynOptics definition for PoE	bayStackPethExt.mib
Rapid City MIB	rapid_city.mib

Table continues…

Proprietary MIB name	File name
Note: The MACsec tables, namely, rcMACSecCATable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	
SynOptics Root MIB	synro.mib

Chapter 20: Resources

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Documentation

See *Documentation Reference* for a list of documentation for all VOSS products.

For installation and initial setup information of the Open Networking Adapter (ONA), refer to the Quick Install Guide that came with your ONA.

 * **Note:**

The ONA works only with the Avaya Virtual Services Platform 4000 Series.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:

  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:

  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.

  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  ✳ **Note:**

  Videos are not available for all products.

Searching a documentation collection

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

Before you begin

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

Procedure

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>*.pdx.

3. In the Search dialog box, select the option **In the index named *<product_name_release>*.pdx**.

4. Enter a search word or phrase.

5. Select any of the following to narrow your search:

   - Whole Words Only

- Case-Sensitive

- Include Bookmarks

- Include Comments

6. Click **Search**.

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

Subscribing to e-notifications

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

About this task

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

Procedure

1. In an Internet browser, go to https://support.avaya.com.

2. Type your username and password, and then click **Login**.

3. Under **My Information**, select **SSO login Profile**.

4. Click **E-NOTIFICATIONS**.

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

GENERAL NOTIFICATIONS

1/5 Notifications Selected

End of Sale and/or Manufacturer Support Notices ☐

Product Correction Notices (PCN) ☑

Product Support Notices ☐

Security Advisories ☐

Services Support Notices ☐

UPDATE »

6. Click **OK**.

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

PRODUCT NOTIFICATIONS   Add More Products

☐ Show Details   **1 Notices**

8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.

11. Click **Submit**.

Glossary

Advanced Encryption Standard (AES)	A privacy protocol the U.S. government organizations use AES as the current encryption standard (FIPS-197) to protect sensitive information.
American Standard Code for Information Interchange (ASCII)	A code to represent 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 specific time interval.
Circuitless IP (CLIP)	A CLIP is often called a loopback and is a virtual interface that does not map to any physical interface.
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 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 and 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 certain 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.
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)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
Layer 1	Layer 1 is the Physical Layer of the Open System Interconnection (OSI) model. Layer 1 interacts with the MAC sublayer of Layer 2, and performs character encoding, transmission, reception, and character decoding.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
Link Aggregation Control Protocol (LACP)	A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.
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)	The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
mask	A bit string that the device uses 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 switch directs the data 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.

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 specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.
Protocol Independent Multicast, Sparse Mode (PIM-SM)	PIM-SM is a multicast routing protocol for IP networks. PIM-SM provides multicast routing for multicast groups that can span wide-area and inter-domain networks, where receivers are not densely populated. PIM-SM sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic. 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)	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more 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. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.
Secure Copy (SCP)	Secure Copy securely transfers files between the switch and a remote station.
Secure Shell (SSH)	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
SFP	A hot pluggable, small form-factor pluggable (SFP) transceiver, which is used in Ethernet applications up to 1 Gbps.
Simple Loop Prevention Protocol (SLPP)	Simple Hello Protocol that prevents loops in a Layer 2 network (VLAN).

Simple Network Management Protocol (SNMP)	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 10 micrometers), with a cladding that is 10 times the core diameter. These fibers have a potential bandwidth of 50 to 100 gigahertz (GHz) per kilometer.
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 receiver-transmitter (UART)	A device that converts outgoing parallel data to serial transmission and incoming serial data to parallel for reception.
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.
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.
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.