ExtremeSwitching™

Administering VOSS

Release 8.2 (VOSS)
9036559-00 Rev AD
November 2020

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

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

- Extreme Networks VSP 4000 Series (includes VSP 4450 Series)
- Extreme Networks VSP 4900 Series
- Extreme Networks VSP 7200 Series
- Extreme Networks VSP 7400 Series
- Extreme Networks VSP 8000 Series (includes VSP 8200 Series and VSP 8400 Series)
- Extreme Networks VSP 8600 Series
- Extreme Networks XA1400 Series

Note:

VOSS is licensed on the XA1400 Series as a Fabric Connect VPN (FCVPN) application, which includes a subset of VOSS features. FCVPN transparently extends Fabric Connect services over third-party provider networks.

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.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product.
🗒	Note	Useful information or instructions.
➡	Important	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon.

Table continues…

Convention	Description
	Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do

Table continues…

Convention	Description
	not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products

- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

   ✱ **Note:**
   You can modify your product selections or unsubscribe at any time.
4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

The following sections detail what is new in this document.

Bidirectional Forwarding Detection over Fabric Extend Tunnels

Bidirectional Forwarding Detection (BFD) provides a fast failure-detection mechanism between peer systems. The peer systems exchange BFD packets, and when one of the systems does not receive a BFD packet after a specific period of time, the system assumes that the link or the other system is not operating, and declares the link down.

BFD functionality on VOSS is extended to support fast failure-detection for Fabric Extend (FE) tunnels.

For more information, see Bidirectional Forwarding Detection on page 461.

Segmented Management

Segmented Management introduces a new way of managing switches running VOSS. With Segmented Management, the Management plane (management protocols) is separated from the Control Plane (routing plane) from a process and data-path perspective. Segmented Management is the only method to manage VOSS switches starting with this release and one or a combination of the management interface/management instance types below can be used:

- Out-of-Band (OOB) management IP address (IPv4 and/or IPv6)
- In-band Loopback/circuitless IP (CLIP) management IP address (IPv4 and/or IPv6)
- In-band management VLAN IP address (IPv4 and/or IPv6)

Segmented Management provides better security since you cannot reach the management instance from outside the VRF (in the case of CLIP) or outside VLAN/I-SID (in the case of management VLAN) and because it has a new built-in firewall for the management plane. There is also more predictability with symmetric traffic flows for management traffic originating from and terminating on the switch.

- Sessions originated from switch (client mode) - Source IP of packets is determined based on Management IP stack routing table weights (configurable).
- Sessions connecting to switch (server mode) - Source IP is derived from session connection and reply will go out on management interface packet.

This feature also introduces new management applications, such as DHCP Client, DHCP option 43 support, RADIUS Security, RMON2, improved Key Health Indicators (KHI) and statistics. Some older management applications such as rsh, rlogin and NTPv3 have been deprecated. Segmented Management also adds IPv6 support for Link Layer Discovery Protocol (LLDP) in this release.

Prior to upgrading to this release with Segmented Management, you must migrate a VLAN and/or CLIP that is dedicated for management use only. The OOB management interface is migrated automatically.

For more information, see Segmented Management on page 400.

Statistics for Segmented Management Instance

Additional management statistics are added for the Segmented Management Instance management interfaces. You can use CLI or EDM to show IP address statistics, ICMP statistics, TCP statistics, TCP connections, UDP connections, and UDP endpoints for all three management interfaces. Clearing management statistics now clears all the IPv4 and IPv6 statistics across all management interfaces simultaneously.

For more information, see the following sections:

- Segmented Management Instance Overview on page 402
- View Segmented Management Instance Statistics on page 424
- View IP ICMP Statistics for a Segmented Management Instance on page 449
- View IP Address Statistics for a Segmented Management Instance on page 446
- View IP Address for a Segmented Management Instance on page 445
- View IPv6 Address for a Segmented Management Instance on page 446
- View IPv6 Operational Routes for a Segmented Management Instance on page 458
- View TCP Connections and UDP Endpoints Statistics for a Segmented Management Instance on page 454
- View TCP Statistics for a Segmented Management Instance on page 453
- View UDP Statistics for a Segmented Management Instance on page 452

Source IP for Segmented Management Instance

The behavior of Source IP packet fluctuations across many management interfaces and routes is changed because the Segmented Management Instance has a maximum of three management interfaces. This release removes the configuration to specify the Source IP for specific management application. The Source IP is now determined by separate routing tables for each Segmented Management Instance interface, plus a default main table. Multiple routing tables are in use, and each management interface can have overlapping or identical static routes without interfering with each other. The main table has a super-set of all routes where the weight of the static route can tie-break routes to the same destination going through different management interfaces. The following default weights and Source IP default route priority is management CLIP, then management VLAN, then management OOB interface:

- mgmt clip - 100

  mgmt vlan - 200

  mgmt oob - 300

You can route packets through a different management interface than the default configuration, but you must add a specific static route or change the default weight of the management interface.

Note:

If you change the default route weight, the management interface with the lowest weight value becomes default route for all segmented management interface traffic.

For more information, see Segmented Management Instance Considerations and Restrictions on page 409.

Topology IP for Segmented Management Instance

Link Layer Discovery Protocol (LLDP) and SynOptics Network Management Protocol (SONMP) behavior is changed for the Segmented Management Instance. Now both LLDP and SONMP advertise the same topology IP address. LLDP now supports both IPv4 and IPv6 advertisement and SONMP supports IPv4 advertisement only. If all three management interfaces are configured, the advertised default topology IP priority is management CLIP, then management VLAN, then management OOB. You can change the default topology IP using CLI or EDM. If a management interface is configured with multiple IPv4 addresses, the advertised IP priority is static IP address, then DHCP IP address, then link-local IP address. You cannot change the advertised IPv4 address priority.

For more information, see the following sections:

- Segmented Management Instance Considerations and Restrictions on page 409
- SynOptics Network Management Protocol on page 137
- Link Layer Discovery Protocol (802.1AB) Fundamentals on page 289
- Configure a Segmented Management Instance Interface as Default Topology IP on page 418
- View Topology IP for a Segmented Management Instance on page 445

DHCP Client for Segmented Management Instance

To support Zero Touch Deployment with ExtremeCloud IQ, this release adds a DHCP Client for the Segmented Management Instance VLAN management interface or Out-of-Band (OOB) management interface. The DHCP Client configuration supports a VLAN mode, OOB mode, and a cycle mode. DHCP Client cycle mode alternates IP address requests between the VLAN management interface and OOB management interface until an IP address is obtained on one of the interfaces.

Note:

The DHCP Client is disabled by default on previously configured or upgraded switches.

The DHCP Client is enabled by default in cycle mode when:

- A manufacturing image is of a version that supports this feature.

  The switch ships directly from manufacturing with VOSS Release 8.1.60 or later.
- The primary and secondary configuration file is not on the switch.
- The primary and secondary configuration file fail to load on the switch.

You can also manually configure the DHCP Client to request an IPv4 address from a DHCP server for the In-band VLAN management interface, or the OOB management interface, or to cycle requests until an IP address is obtained on a VLAN or OOB management interface. The DHCP Client supports IPv4 addresses only, and cannot be enabled on multiple management interfaces simultaneously.

For more information, see the following sections:

- DHCP Client on page 407
- Segmented Management Instance Considerations and Restrictions on page 409
- Configure the DHCP Client for a Segmented Management Instance on page 416

- Configure DHCP Client for a Segmented Management Instance on page 438

For more information about DHCP Client, see

Rlogin Deprecation

Remote login (rlogin) is no longer supported on the switch.

For more information, see: Access Policies for Services on page 513

NTPv3 Deprecation

Network Time Protocol version 4 (NTPv4) is now the only supported version of NTP on the switch. Existing NTPv3 configurations automatically migrate to NTPv4 with no additional configuration required.

Ping and Traceroute Enhancements

This release allows the use of ping and traceroute in the following context:

- Global Routing Table context (GRT)
- Management context (mgmt)
- VRF context (VRF)

The default value for the default ping and traceroute command context is GRT.

For more information, see:

- Ping an IP Device on page 46

Zero Touch Deployment

Zero Touch Deployment enables a VOSS switch to be deployed automatically with ExtremeCloud IQ but you still must onboard the switch on the ExtremeCloud IQ side. When the switch powers on, the DHCP Client obtains the IP address and gateway from the DHCP Server, and discovers the Domain Name Server, connecting the switch automatically to Extreme Management Center or to ExtremeCloud IQ cloud management applications.

To use zero touch functionality, your switch must be in a Zero Touch Deployment-ready configuration mode, which means the switch cannot have existing primary or secondary configuration files loaded. Factory shipped switches are Zero Touch Deployment ready because they deploy without configuration files. However, existing switches require manual preparation before Zero Touch Deployment can function.

For more information, see the following sections:

- Boot Sequence on page 72
- Zero Touch Deployment on page 77
- Configuration Considerations on page 78

Notice about Feature Support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not display on your hardware, it is not supported.

For information about physical hardware restrictions, see your hardware documentation.

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 Series 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 Series 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 Configuring User Interfaces and Operating Systems for VOSS.

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 Series, 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 Series (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.

Before You Upgrade

This section provides important feature impacts you need to understand before you upgrade the switch software.

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 for VOSS for interoperability considerations.

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 the following: 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 the following: direct, ospf, static, rip or bgp.

Important upgrade consideration regarding MACsec

The switch software does not support the replay-protect option when MACsec is configured with static security keys. 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 and you are upgrading to switch software configured with MACsec using static security keys, follow the steps below to disable replay-protect before you upgrade the switch software to a release where the option is not available.

Beginning in Release 8.1, replay protection is available as part of the MACsec Key Agreement (MKA) feature on the VSP 8404 and VSP 8404C platforms. For platforms that do not support MKA, disable replay protection.

Note:

Replay-protect must be 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. We recommend that you complete the following procedure before initiating the upgrade.

Procedure

1. To check if replay-protect has been enabled on any of the interfaces, use the **`show macsec status`** command.

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

Table 3: nni-mstp boot flag product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
nni-mstp boot flag (**`boot config flags nni-mstp`**) **Important:** This flag has special upgrade considerations the first time you upgrade to a release that supports it.	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

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.
```

TACACS+ upgrade consideration

When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

Note:

This issue affects upgrades from VOSS 4.1.X only. It does not affect upgrades from VOSS 4.2 or higher.

VLAN and MLT Upgrade Considerations

VLAN or MLT Name Uses all Numbers

Representational State Transfer Configuration Protocol (RESTCONF) does not allow VLAN or MLT names that contain all numbers. Beginning with VOSS 8.0, the VLAN or MLT name cannot use all numbers. If, in a release prior to 8.0, you configured a name that was all numbers, see the following table to understand the impact of upgrading to a newer release.

Table 4: Upgrade impact on interface names with all numbers

Target upgrade release	Impact after upgrade
VOSS 8.0.5.x, 8.0.6.x, or 8.0.7.x	The system prepends VLAN- or MLT- , and appends -01, to the name during the upgrade. For example, the VLAN name 222 becomes VLAN-222-01.
VOSS 8.0.8 and later	If you plan to enable RESTCONF, you must check interface names for invalid special characters or conflicts, and make necessary modifications manually. For information about how to check interface names, see the RESTCONF content in Configuring User Interfaces and Operating Systems for VOSS.
VOSS 8.1 or 8.1.1.x	The system prepends VLAN- or MLT- , and appends -01, to the name during the upgrade. For example, the VLAN name 222 becomes VLAN-222-01.
VOSS 8.1.2 and later	If you plan to enable RESTCONF, you must check interface names for invalid special characters or conflicts, and make necessary modifications manually. For information about how to check interface names, see the RESTCONF content in Configuring User Interfaces and Operating Systems for VOSS.

Extreme Integrated Application Hosting Virtual Service Upgrade Considerations

Virtual Service and vport Name Length Change

In VOSS 8.0.5, the length of the virtual service name and vport name changed to 80 and 32 characters respectively. If, in a release prior to 8.0.5, you configured a name with length that exceeds the new value, you must change the name before you upgrade to 8.0.5 or later.

If you do not change the name prior to upgrade, the virtual service configuration will not pass a consistency check in VOSS 8.0.5 and later, and the configuration will not be loaded. You will need to modify your configuration to comply with the new name lengths and reload it for the virtual service to load.

IPFIX Upgrade Considerations

In VOSS 8.0.5, the range for the IPFIX aging interval changed from <1-1800> to <1-60>. If, in a release prior to 8.0.5, you configured the aging interval to be greater than 60 seconds and you upgrade to 8.0.5 or later, your configuration will be updated to 60 seconds.

Zero Touch Fabric Configuration Upgrade Considerations

The following releases included modified Zero Touch Fabric Configuration support that impacts upgrades from earlier releases:

- VOSS 7.1.3 and later
- VOSS 8.0.6 and later
- VOSS 8.1 and later

Considerations if Upgrading from a Release without Zero Touch Fabric Configuration Support

Check the Intermediate System-to-Intermediate System (IS-IS) manual area using the **`show isis manual-area`** command to determine if the manual area equals `00.1515.fee1.900d.1515.fee1.900d`.

The manual area `00.1515.fee1.900d.1515.fee1.900d` is the normal area ID before you upgrade. After you upgrade, the switch triggers the Zero Touch Fabric Configuration procedures.

To keep the existing switch behavior and not use Zero Touch Fabric Configuration, change the IS-IS manual area to a value other than `00.1515.fee1.900d.1515.fee1.900d` before you upgrade.

Note:

If IS-IS is the management network used to reach the node and you do not change the manual area before you upgrade, the node will not form an IS-IS adjacency after the upgrade and will not join the network.

Considerations if Upgrading from a Release with Zero Touch Fabric Configuration Support

Check the IS-IS manual area using the **`show isis manual-area`** command to determine if the manual area equals `00.0000.0000` or is a `00` of any length.

`00.0000.0000` is the area ID that triggers Zero Touch Fabric Configuration before the upgrade. This area ID will not trigger Zero Touch Fabric Configuration after the upgrade.

To keep the existing switch behavior of using Zero Touch Fabric Configuration, change the IS-IS manual area to `00.1515.fee1.900d.1515.fee1.900d` before you upgrade. After you upgrade, the switch triggers the Zero Touch Fabric Configuration procedures.

Note:

If IS-IS is the management network used to reach the node and you do not change the manual area before you upgrade, the node will not form an IS-IS adjacency after the upgrade and will not join the network.

If you do not want Zero Touch Fabric Configuration procedures to run after the upgrade, ensure the IS-IS manual area is a value other than `00.1515.fee1.900d.1515.fee1.900d` before you upgrade.

Digital Certificate Upgrade Considerations

Public Key Length

To support SNMP walk for rcDigitalCertTable where the public key length exceeds 2,048 characters, VOSS 8.1 and later configures MAX_KEY_LEN to 2,048 to extend PublicKey to hold a maximum of 4,096-bit key. After this key length is updated, the format for `/intflash/.cert/cert_info.cfg` changes based on the new public key maximum length and you will be unable to restore the CertInfoTable from this file.

If you upgrade to VOSS 8.1 or later from an earlier release, you must reconfigure the certificates because you cannot restore the old certificate configuration after reboot.

The switch displays the following log message after you upgrade to VOSS 8.1, or later, and reboot:

```
GlobalRouter DIGITALCERT ERROR Unable to restore info from /
intflash/.cert/cert_info.cfg due to different/wrong format
```

Fast PoE and Perpetual PoE Upgrade Considerations

When you upgrade from VOSS 8.1.X to VOSS 8.1.5, the POE Controller undergoes a firmware update, which reverts previously configured Fast PoE and Perpetual PoE settings back to the default values. The system displays a message to inform you about this change.

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.

Note that not all CLI commands are included in configuration files. Typical examples include, but are not limited to some operational and security-related commands.

Note:

When loading large configuration files or large sections of a configuration file, avoid copying and pasting of the files into the console or terminal window as it can lead to the loss of configuration. You must either source the file or boot to the intended configuration file. Sourcing and booting allow for the debug and verification of the configuration file using the boot config flags. For more information about booting, sourcing, and debugging or verification using boot flags, see Command Line Interface Commands Reference for VOSS.

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

The following table defines parameters for 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.

Table continues…

Variable	Value
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

Important:

Upgrades from some releases require release-specific steps. For more information, see Release Notes for VOSS.

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:

  Product Notice: For VSP 4850 Series, 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 Series (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation.

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

For information about how to remove a software release, see Deleting a software release on page 39.

Before you begin

- To obtain the new software, go to the Extreme Networks support site: http://www.extremenetworks.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 27.
- 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.

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 applies to all 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

The following table defines parameters for 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
```

Update the Complex Programmable Logic Device (CPLD) Image

✱ **Note:**

This procedure only applies to VSP 4900 Series.

During the device bootup, if an older version of a CPLD module is detected, the system displays a log message to recommend you upgrade the CPLD module image.

The following is an example of the log message:

```
1 2020-01-17T13:08:16.630Z VSP-4900-12MXU-12XE CP1 - 0x0026050d -
00000000 GlobalRouter SW INFO cpu CPLD/FPGA module is running older
version. Recommeded to upgrade using command cpld-install.
```

You can also use **`show sys-info cpld`** command to check the current version of the CPLD module on the device.

Before you begin

Upgrade the software on the switch to the latest build.

About this task

The **`cpld-install`** command compares the image version of the modules with their current version on the device:

- If the versions are the same, the command exits.
- If the current version is an earlier version, you must update the image version of the specific module.

The device automatically restarts after sucessful installation of the specific module.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Update one of the following CPLDs:
   - CPU:

     ```
     cpld-install cpu [WORD<1-99>]
     ```

   - Field-Programmable Gate Array (FPGA):

     ```
     cpld-install fgpa [WORD<1-99>]
     ```

   - Port:

     ```
     cpld-install port [WORD<1-99>]
     ```

   - VIM (Versatile Interface Module):

     ```
     cpld-install vim [WORD<1-99>]
     ```

3. When prompted, type `y` to continue with the CPLD update.

Example

Update CPLD for port module.

```
Switch:1>cpld-install port /intflash/1.1.8_sd_portpld.tgz
image file md5 checksum passed
Current port CPLD version is 0x1108, 1.1.08

Do you want to continue with cpld update? (y/n) ? y

 WARNING: Upgrading FPGA requires writing to a device
```

```
 WARNING: It will take about a minute or so to complete.

 WARNING: DO NOT TURN POWER OFF OR MAKE ANY HARDWARE CHANGES ONCE YOU START THIS OPERATION.

FPGA upgrade completed successfully

System is going for powercycle now...
1 2019-12-13T14:55:55.577+05:30 VSP-4900-24S CP1 - 0x0026050c - 00000000 GlobalRouter SW INFO port CPLD
update completed successfully.
CP1  [12/13/19 14:55:56.000] LifeCycle: INFO: Stopping all  processes
Switch:1>CP1  [12/13/19 14:56:01.000] LifeCycle: INFO: Process slamon.sh (pid:20748) stopping with
signal 9
1 2019-12-13T14:56:01.225+05:30 VSP-4900-24S CP1 - 0x0000c5f9 - 00000000 GlobalRouter HW INFO Link
Down(1/14). Port is disabled
1 2019-12-13T14:56:01.226+05:30 VSP-4900-24S CP1 - 0x00004726 - 00000000 GlobalRouter SNMP INFO SPBM
detected adj DOWN on Port1/14,
neighbor 489b.d59d.6884 (VSP-4900-12MXU-12XE)
1 2019-12-13T14:56:01.226+05:30 VSP-4900-24S CP1 - 0x00000033 - 00000000 GlobalRouter SW ERROR
dpmSendMulti: LtrSend Failed: Status=9
1 2019-12-13T14:56:01.226+05:30 VSP-4900-24S CP1 - 0x000e05dc - 00000000 GlobalRouter HAL ERROR
dpmCosqProfileApply: request ltrSend FAILED
1 2019-12-13T14:56:01.229+05:30 VSP-4900-24S CP1 - 0x0000c5f9 - 00000000 GlobalRouter HW INFO Link
Down(1/24). Port is disabled
1 2019-12-13T14:56:01.233+05:30 VSP-4900-24S CP1 - 0x00010756 - 0040000b.3 PERSISTENT SET GlobalRouter
HW WARNING Module VSP4900-24S in slot 1
is non-operational
1 2019-12-13T14:56:01.267+05:30 VSP-4900-24S CP1 - 0x00000033 - 00000000 GlobalRouter SW ERROR
dpmSendMulti: LtrSend Failed: Status=9
1 2019-12-13T14:56:01.267+05:30 VSP-4900-24S CP1 - 0x000e05dc - 00000000 GlobalRouter HAL ERROR
dpmSendMacAddrDelMsg: request ltrSend FAILED
1 2019-12-13T14:56:01.267+05:30 VSP-4900-24S CP1 - 0x00100665 - 00000000 GlobalRouter SW WARNING
dpmDeleteMacAddress: failed for
Mac = 02:78:84:ff:ff:ff, Mgid = 4052
1 2019-12-13T14:56:01.271+05:30 VSP-4900-24S CP1 - 0x000646fa - 00000000 GlobalRouter MLT INFO IST DOWN,
status vector: 0x60000000001800
1 2019-12-13T14:56:01.271+05:30 VSP-4900-24S CP1 - 0x000646da - 01900004 DYNAMIC SET GlobalRouter MLT
WARNING SMLT IST Link is DOWN /IST Slave
CP1 [12/13/19 14:56:04.000] LifeCycle: INFO: Stopped all processes
CP1 [12/13/19 14:56:04.000] LifeCycle: INFO: All processes have stopped
CP1 [12/13/19 14:56:04.000] LifeCycle: INFO: Setting shutdown countdown to 300 seconds
CP1 [12/13/19 14:56:04.000] LifeCycle: INFO: Flushing buffers ... OK
CP1 [12/13/19 14:56:04.000] LifeCycle: INFO: Restarting module
CP1 [12/13/19 14:56:05.000] LifeCycle: INFO: Powercycling the system!
Using device type 1 (FPGA)
RECONFIGURE command enabled
Lock file name is /tmp/FPGA_lock
FPGA RECONFIGURE operation started.
FPGA RECONFIGURE operation SUCCEEDED.
```

Variable Definitions

The following table defines parameters for the **`cpld-install`** command.

Variable	Value
cpu	Updates the CPU module.
fpga	Updates the FPGA module.
port	Updates the Port module.
vim	Updates the VIM module.
WORD<1-99>	Specifies the image filename.

Table continues…

Variable	Value
	Note: This parameter is optional. If you do not specify the filename the command checks .tgz file for the image from the running VOSS filesystem.

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

The following table defines parameters for 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 Configuring User Interfaces and Operating Systems for VOSS.

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

The following table defines parameters for 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

The following table defines parameters for 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
```

Ping 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 displays 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.

Ping and traceroute can fail for VRF routes if you use large packet sizes for the operation. Do not use packet sizes larger than the following:

- Ping for VRF: 1480 bytes
- Traceroute for VRF: 1444 bytes

Note:

Exception: large packets for VRF routes are supported on the CLIP Segmented Management Instance.

A management instance ID can be specified to enable the system to use the correct source for the outgoing ICMP ECHO request packet.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Ping an IP network connection:

   ```
   ping WORD<0-256> [-d] [-I <1-60>] [-s] [-t <1-120>] [count <1-9999>]
   [datasize <28-9216|28-51200>] [grt] [interface gigabitEthernet
   {slot/port[sub-port]}|mgmtEthernet mgmt | tunnel <1-2000> | vlan
   <1-4059>] [scopeid <1-9999>] [source WORD<1-256>] [vrf WORD<1-16>]
   ```

Note:

The mgmtEthernet mgmt parameter is only supported on VSP 8600 Series.

Note:

The grt parameter is not supported on VSP 8600 Series.

3. Ping an IP network connection using a Global Routing Table (GRT):

```
ping WORD<0-256> [-d] [-I <1-60>] [-s] [-t <1-120>] [count <1-9999>]
[datasize <28-9216|28-51200>] grt [interface gigabitEthernet {slot/
port[sub-port]}| tunnel <1-2000> | vlan <1-4059>][source
WORD<1-246>]
```

4. Ping a network connection using a Segmented Management Instance:

```
ping WORD<0-256> [-s] [-t <1-120>] [count <1-9999>] [datasize
<28-9216|28-51200>] mgmt [clip | oob | vlan]
```

Note:

If you do not use the mgmt parameter, the **`ping`** command uses the VOSS IP routing stack to initiate the ping request.

Note:

If you ping a device using a management CLIP, the ping source IP address is configured as the management CLIP IP address. If you ping a device using a management VLAN, the ping source IP address is configured as the management VLAN IP address.

Example

Ping an IP device from a GRT VLAN IP interface:

```
Switch:1#ping 192.0.2.16 grt interface vlan 1
192.0.2.16 is alive
```

Ping a device using the management routing table:

```
Switch:1#ping 192.0.2.12 mgmt
```

Ping a device using a management CLIP:

```
Switch:1#ping 192.0.2.12 mgmt clip
```

Ping an IP device using a management VLAN:

```
Switch:1#ping 192.0.2.12 mgmt vlan
```

Variable Definitions

The following table defines parameters for the **`ping`** command.

Variable	Value
count <1–9999>	Specifies the number of times to ping. The default is 1.

Table continues…

Variable	Value
-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). This parameter does not apply if you use the mgmt [clip | oob | vlan] parameter.
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 64.
grt	Specifies the ping in Global Routing Table context.
-I <1–60>	Specifies the interval between transmissions in seconds.
interface *gigabitEthernet {slot/port[sub-port]}| mgmtEthernet mgmt| tunnel <1–2000>* | *vlan <1-4059>*	Specifies the outgoing interface. Additional ping interface parameters: • gigabitEthernet {slot/port[sub-port]}: gigabitethernet port • mgmtEthernet mgmt: identifies the physical management port **Note:** mgmtEthernet is only supported on VSP 8600 Series. • tunnel: tunnel ID as a value from 1 to 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. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. This parameter does not apply if you use the mgmt [clip | oob | vlan] parameter.
mgmt [clip | oob | vlan]	Specifies the Segmented Management Instance as the source for the outgoing ICMP ECHO packet. The packet goes out this specific interface only.

Table continues…

Variable	Value
	If you do not specify the management interface type, the **ping** command uses the management routing table to determine the best management interface and selects the source IP based on the egress management interface. ✱ **Note:** The **vlan** and **oob** parameters are not supported on VSP 8600 Series. For more information about feature support, see VOSS Feature Support Matrix.
-s	Configures the continuous ping at the interval rate defined by the [-I] parameter or until you enter a **Ctrl + C** keystroke.
scopeid *<1–9999>*	Specifies the circuit ID for IPv6. This parameter does not apply if you use the mgmt [clip | oob | vlan] parameter.
source *WORD<1-256>*	Specifies the source IP address for the ping command. This parameter does not apply if you use the mgmt [clip | oob | vlan] parameter.
-t <1–120>	Specifies the no-answer timeout value in seconds. The default is 5.
WORD<0–256>	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address.
vrf WORD<1–16>	Specifies the virtual router and forwarder (VRF) name. This parameter does not apply if you use the mgmt [clip | oob | vlan] parameter.

Configure the Default Ping and Traceroute Context

About this task

Ping commands and traceroute commands execute in Global Router (GRT) context by default. You can configure ping commands and traceroute commands to execute in management (mgmt) context or in Virtual Router Forwarding (vrf) context.

✱ **Note:**
This procedure is not supported on VSP 8600 Series.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure the default ping command and traceroute command context:

```
sys default-ping-context {grt | mgmt | vrf}
```

Variable Definitions

The following table defines parameters for the **sys default-ping-context** command.

Note:
The **sys default-ping-context** command is not supported on VSP 8600 Series.

Variable	Value
grt	Specifies Global Routing Table (grt) context as the default context for ping commands and traceroute commands. The default configuration is grt as the default context.
mgmt	Specifies management (mgmt) context as the default context for ping commands and traceroute commands. The default configuration is grt as the default context.
vrf	Specifies Virtual Router Forwarding (vrf) context as the default context for ping commands and traceroute commands. The default configuration is grt as the default context.

Calculating and Verifying the MD5 Checksum for a File on the Switch

Perform this procedure to verify that the software files are downloaded properly to the switch. The MD5 checksum for each release is available on the Extreme Networks Support website.

About this task

Calculate and verify the MD5 checksum after you download software files.

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.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View the list of files:

```
ls *.tgz
```

3. Calculate the MD5 checksum for the file:

```
file-checksum md5 WORD<1-99>
```

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 a process that can be used on all VOSS 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>file-checksum md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.0.0.0.tgz) = 80bfe69d89c831543623aaad861f12aa
```

Variable Definitions

The following table defines parameters for the **`file-checksum md5`** command:

Variable	Value
WORD<1-99>	Specifies the file name.

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. The MD5 checksum for each release is available on the Extreme Networks 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 displays a process that applies to software files for all VOSS 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 File Checksum

About this task

Perform the following procedure to calculate or comapre the MD5 or SHA512 digest for a specific file. The **file-checksum** command calculates the MD5 or SHA512 digest for files on the internal flash and either shows the output on screen or stores the output in a file that you specify. The **file-checksum** command compares the calculated MD5 or SHA512 digest with that in a checksum file on flash, and the compared output appears on the screen. By verifying the MD5 or SHA512 checksum, you can verify that the file is transferred properly to the switch.

Important:

- If the MD5 key file parameters change, you must remove the old file and create a new file.
- Use the **file-checksum** command with reserved files (for example, a password file) only if you possess sufficient permissions to access these files.

Procedure

1. To enter User EXEC mode, log on to the switch.

2. Calculate the file checksum:

   ```
   file-checksum {md5 | sha512} WORD<1-99> [-a] [-c] [-f WORD<1-99>] [-r]
   ```

Example

```
Switch:1>file-checksum md5 password -a -f password.md5
```

Variable Definitions

The following table defines parameters for the **`file-checksum`** command.

Variable	Value
md5	Calculates or compares the MD5 digest for a specific file.
sha512	Calculates or compares the SHA512 digest for a specific file.
-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 with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum filename is not specified, the file `/intflash/checksum.md5` is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: Error: Checksum file <*filename*> not present. The -c option also • calculates the checksum of the specified files • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison
-f	Stores the result of MD5 checksum to a file on internal flash. If the output file specified with the -f option is reserved filenames on the switch, the command fails with the error message: `Error: Invalid operation.`

Table continues…

Variable	Value

	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.
WORD<1–99>	Specifies the file name.

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

The following table defines parameters for 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

Source a configuration to merge a script file into the running configuration or verify the syntax of a configuration file.

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. Use the source command to merge smaller portions of a configuration into the existing configuration.

Not all CLI commands are included in configuration files. Typical examples include, but are not limited to some operational and security-related commands. Ensure that you understand what configuration options are included or not included in a configuration file, when you use that file to build new configurations.

The operational modes in the boot configuration file must be configured for some features (for example, **`spbm-config-mode true/false`**). Before sourcing a configuration file, you need to configure the **`boot config flag`**, save the configuration, and reboot the system. After the reboot, you can source the configuration file without fail.

Important:

Do not source a verbose configuration (verbose.cfg) with the debug stop option. The sourcing process cannot complete if you use these two options with a verbose 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

The following table defines parameters for the **source** command.

Variable	Value
debug	Debugs the script by outputting the configuration commands to the screen.
stop	Stops the sourcing of a configuration if an error occurs.
syntax	Checks the syntax of the configuration file. This parameter does not load the configuration file; only verifies the syntax. If you use this parameter with the stop parameter (**source WORD<1-99> stop syntax**), the output appears on screen and verification stops if it encounters an error. If you use this parameter with the debug parameter (**source WORD<1-99> debug syntax**), the output does not stop if it encounters an error; you must review the on-screen output to verify if an error exists. If you use this parameter by itself, it does not output to the screen or stop on error; it shows an error message, `syntax errors in script`, to indicate if errors exist in the configuration file.
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.

Using the USB device

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

Important:

Product Notice: For VSP 4850 Series, 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 Series (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

The following table defines parameters for 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.

Table continues…

Variable	Value
`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

The following table defines parameters for 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

The following table defines parameters for 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

The following table defines parameters for 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

The following table defines parameters for the `delete` command.

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

Back Up Configuration Files to ZIP

Table 5: Extreme Management Center backup configuration ZIP file product support

Feature	Product	Release introduced
Extreme Management Center backup configuration ZIP file For more information, see Extreme Management Center documentation.	VSP 4450 Series	VOSS 6.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.1.2
	VSP 8400 Series	VOSS 6.1.2

Table continues…

Feature	Product	Release introduced
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50

Extreme Management Center (XMC) has a configuration backup feature with a requirement to be able to backup configuration related files. Release 6.1.2 introduces new CLI commands to backup configuration related files and package them into a single zip file, or to restore configuration files that were backed up.

Note:

License files are not backed up.

Backing up configuration files to a ZIP file

About this task

Use this procedure to back up configuration files.

Important:

Only the RWA user can use the **backup** command.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Use the backup command:

   ```
   backup configure WORD<1-99>
   ```

Example

```
Switch:1>enable
Switch:1#backup configure /intflash/backup02072018

Successfully backed up config /intflash to /intflash/backup02072018.tgz
```

Restoring configuration files from a ZIP file

About this task

Use the following procedure to restore previously backed up configuration files.

Before you begin

- Download the backup file to the /intflash directory.
- If restoring the configuration files on a new switch, you must do one of the following:
  - Disable ISIS on the old switch .
  - Power the old switch down.
  - Remove the old switch from the network.
- If restoring the configuration files on a different switch, use the “isis dup-detection-temp-disable “ command on the new switch to suspend duplicate detection prior to its insertion into the existing SPBM topology.

Important:

This must be done after the original unit has been completely removed or isolated from the SPBM topology.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Run the restore command to restore the configuration files.

   ```
   restore configure WORD<1-99>
   ```

Example

```
Switch:1>enable
Switch:1#restore configure /intflash/backup02072018.tgz

Warning: Command will restore your backup setup and access files
  The current files will be overwritten.

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

 Restore /intflash from /intflash/backup02072018.tgz is complete!
 Reboot is required for the new configuration to be effective
```

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).

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

Show 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 **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click on the **Chassis** tab.
5. Verify the selection for the MTU size.

Display 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 **Configuration** > **Edit**.
2. Click **File System**.
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.

Display 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 **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Flash Files** tab.

Flash Files field descriptions

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

Name	Description
Slot	Specifies the slot number.
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.

Display 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 **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

USB Files field descriptions

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

Name	Description
Slot	Specifies the slot number 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.

Copy a File

About this task

Copy files on the internal flash.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Copy File** tab.
4. Edit the fields as required.
5. Click **Apply**.

Copy File Field Descriptions

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

Name	Description
Source	Identifies the device and file name to copy. You must specify the full path and filename, for example, `<deviceip-ftp server>:/<filename>`
Destination	Identifies the location to which to copy the source file with the filename, for example, `/intflash/<filename>`
Action	Starts or stops the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

Save 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 **Configuration** > **Edit**.
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.

advanced-feature-bandwidth-reservation Boot Flag

Table 6: Advanced Feature Bandwidth Reservation product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Advanced Feature Bandwidth Reservation **Note:** If your switch does not have this boot flag, it is because the hardware reserves the bandwidth automatically with no user interaction.	VSP 4450 Series	Not Supported
	VSP 4900 Series	Not Supported
	VSP 7200 Series	Not Supported
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	Not Supported
	VSP 8400 Series	Not Supported
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.0.50 XA1480 only- demonstration feature

Use the `boot config flags advanced-feature-bandwidth-reservation` command to enable advanced features on the switch. If the `boot config flags advanced-feature-bandwidth-reservation` command is disabled and you attempt to enable an advanced feature, the switch displays an error message to explain why the advanced feature failed to start, and to remind you that you must enable this boot flag for that advanced feature.

Important:

If you change the configuration, you must save the configuration, and then reboot the switch for the change to take effect.

VSP 7400 Series

When disabled, you can use all ports for Layer 2 or Layer 3 forwarding of standard unicast and multicast features. Use this mode if you are not configuring advanced features. The syntax for disabling this boot configuration flag is no boot config flags advanced-feature-bandwidth-reservation.

When enabled, also known as Full Feature mode, the switch supports advanced features by reassigning some of the front panel ports to be loopback ports. The following advanced features require loopback ports:

- Fabric Extend
- SPB
- SMLT
- vIST
- VXLAN Gateway
- Fabric RSPAN (Mirror to I-SID)
- Application Telemetry
- IS-IS Accept Policies

Note:

Full Feature mode does not support PIM.

The syntax for enabling the boot flag for this mode is: **`boot config flags advanced-feature-bandwidth-reservation [low | high]`**.

The high level means that the switch reserves the maximum bandwidth for the advanced features.

The low level means that the switch reserves less bandwidth to support minimum functionality for advanced features.

After the switch reserves the appropriate ports to become loopback ports, the ports are no longer visible in the output when you enter **`show interfaces gigabitEthernet`**.

The following list identifies ports reserved as loopback ports:

- VSP 7432CQ
  - Low reserves ports 1/31 and 1/32.
  - High reserves ports 1/29, 1/30, 1/31, and 1/32.
- VSP 7400-48Y
  - Low reserves ports 1/55 and 1/56.
  - High reserves ports 1/53, 1/54, 1/55, and 1/56

Important:

You must ensure your configuration does not include reserved ports before you enable this feature. If the configuration includes reserved ports after you enable this feature and restart the switch, the switch aborts loading the configuration.

XA1400 Series

Product Notice: This feature is available in demo mode only on XA1480 and supports low configuration automatically, which cannot be modified.

When disabled, all I-SID bindings are removed and the switch can only operate as a Backbone Core Bridge (BCB). The syntax for disabling this boot configuration flag is: **`no boot config flags advanced-feature-bandwidth-reservation`**.

When enabled, the switch reserves CPU cores for Backbone Edge Bridge (BEB) functionality. The syntax for enabling the boot flag for this mode is: **`boot config flags advanced-feature-bandwidth-reservation low`**.

spbm-config-mode boot flag

Table 7: spbm-config-mode product support

Feature	Product	Release introduced
For configuration details, see Configuring Fabric Basics and Layer 2 Services for VOSS.		
spbm-config-mode (**`boot config flags spbm-config-mode`**)	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported

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, the software uses a boot flag called **`boot config flags spbm-config-mode`**.

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

Important:

After you change the **`boot config flags spbm-config-mode`** flag, you must save the configuration, and then 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 for VOSS.

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

Table 8: Linux kernel version product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Linux kernel version	VSP 4450 Series	4.9 as of VOSS 7.0
	VSP 4900 Series	4.14 as of VOSS 8.1
	VSP 7200 Series	4.9 as of VOSS 7.0

Table continues…

Feature	Product	Release introduced
Important: For VSP 4450 Series, VSP 7200 Series, VSP 8200, and VSP 8400 Series, kernel version 4.9 has special upgrade considerations the *first* time you upgrade to a release that supports it. You must first upgrade to a stepping-stone release, 6.1.x , *before* you upgrade to the release with the new kernel.	VSP 7400 Series	4.14 as of VOSS 8.0
	VSP 8200 Series	4.9 as of VOSS 7.0
	VSP 8400 Series	4.9 as of VOSS 7.0
	VSP 8600 Series	4.9 as of VSP 8600 8.0
	XA1400 Series	4.14 as of VOSS 8.1

The switch goes through a 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:

- Loading Linux on page 74
- Loading the Primary Release on page 75
- Deploying Zero Touch on page 75
- Loading the Configuration File on page 75

The following figure shows a summary of the boot sequence.

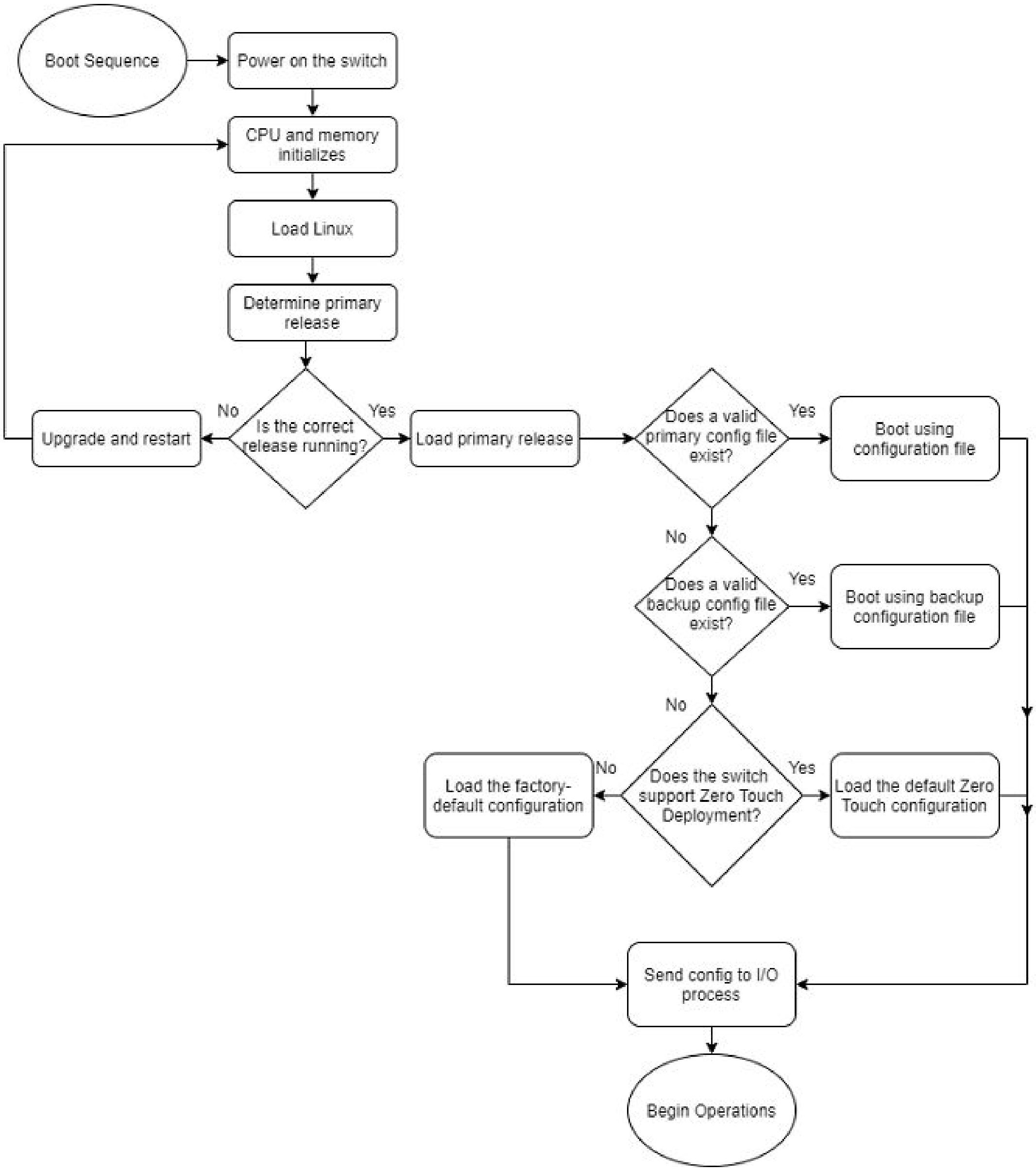

Boot Sequence
Power on the switch
CPU and memory initializes
Load Linux
Determine primary release
Is the correct release running?
No
Yes
Upgrade and restart
Load primary release
Does a valid primary config file exist?
Yes
Boot using configuration file
No
Does a valid backup config file exist?
Yes
Boot using backup configuration file
No
Does the switch support Zero Touch Deployment?
No
Load the factory-default configuration
Yes
Load the default Zero Touch configuration
Send config to I/O process
Begin Operations

Figure 1: Boot Sequence

Loading Linux

Depending on the Linux kernel used, the boot image is stored either in a boot flash partition, Secure Digital (SD), or Solid State Drive (SSD) flash card. The boot image includes the boot loader, and the Linux kernel and applications.

The boot location 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.

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.

Deploying Zero Touch

After the system loads the primary release and the switch is in a Zero Touch Deployment-ready configuration mode, the switch automatically deploys without intervention.

For more information, see Zero Touch Deployment on page 77.

Loading the Configuration File

Important:
The following process only applies if you do not deploy your switch with Zero Touch Deployment functionality. Zero Touch Deployment does not function if primary or secondary configuration files exist.

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 80.

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 9: 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. Use the `boot config flags factorydefaults`.

  Note:

  Zero Touch Deployment does not execute on a switch returned to factory default settings in this manner.

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.

Note:
rlogin is only supported on VSP 8600 Series.

Important:

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

Zero Touch Deployment

Table 10: Zero Touch Deployment product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Zero Touch Deployment	VSP 4450 Series	VOSS 8.2
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	VOSS 8.2
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not supported
	XA1400 Series	VOSS 8.2

For the most current information on switches supported by ExtremeCloud™ IQ, see ExtremeCloud™ IQ Learning What's New.

Zero Touch Deployment enables a VOSS switch to be deployed automatically with ExtremeCloud IQ but you still must onboard the switch on the ExtremeCloud IQ side. When the switch powers on, the DHCP Client obtains the IP address and gateway from the DHCP Server, and discovers the Domain Name Server, connecting the switch automatically to Extreme Management Center or to ExtremeCloud IQ cloud management applications.

Zero Touch Provisioning Plus (ZTP+) provides Extreme Management Center connectivity to VOSS switches.

For more information about IQAgent and ZTP+, see Configuring User Interfaces and Operating Systems for VOSS.

To use zero touch functionality, your switch must be in a Zero Touch Deployment-ready configuration mode, which means the switch cannot have existing primary or secondary configuration files loaded. Factory shipped switches are Zero Touch Deployment ready because they deploy without configuration files. However, existing switches require manual preparation before Zero Touch Deployment can function.

To prepare an existing switch for Zero Touch Deployment, you must do one of the following:

- Delete the existing primary and secondary configuration files.
- Rename existing primary and secondary configuration files. Use the `mv` command to rename the existing configuration files. For example, `mv config.cfg config.cfg.backup`.
- Boot from non-existent configuration files. Use the `boot config choice primary config-file` or `boot config choice primary backup-config-file` commands. For example, `boot config choice primary config-file notafile.cfg` and `boot config choice primary backup-config-file notafile.cfg`.

Configuration Considerations

The switch configuration depends on whether you use factory default mode or Zero Touch Deployment.

Zero Touch Deployment Configuration

With Zero Touch Deployment, the switch configuration consists of the following:

- The ssh and sshd boot configuration flags are enabled by default.
- All ports are Private VLAN isolated ports, except on the XA1400 Series.
- VLAN 4048 is created as an *onboarding-vlan* for host-only connectivity for In Band management. On all other platforms, except the XA1400 Series, all front panel ports are members of VLAN 4048.
- In Band management is enabled.
- DHCP client requests are cycled between In Band and Out of Band ports, except on the XA1400 Series and VSP 4450 Series. XA1400 Series and VSP 4450 Series support In Band management only.
- Out of Band management is enabled, except on the XA1400 Series and VSP 4450 Series. XA1400 Series and VSP 4450 Series support In Band management only.
- All ports are administratively enabled, except on the XA1400 Series. Only Port 1/8 is adminstratively enabled on the XA1400 Series, which means the administrator must plug in and use only port 1/8 for Zero Touch Deployment on an XA1400 Series.
- IQAgent is enabled by default.

  For information about IQAgent, see Configuring User Interfaces and Operating Systems for VOSS.

Factory Default Mode

The switch continues to support the boot configuration flag **`boot config flags factorydefaults`** to return an existing switch to factory default settings.

Note:

Zero Touch Deployment does not execute on a switch returned to factory default settings in this manner.

With the factory default mode, the switch configuration consists of 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 80.

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 Configure Boot Flags on page 98.

Note:

Flag support can vary across hardware models.

Table 11: Boot config flags

CLI flag	Restart
advanced-feature-bandwidth-reservation	Yes
block-snmp	No
debug-config	Yes
debugmode	Yes
dvr-leaf-mode	Yes
enhancedsecure-mode	Yes
factorydefaults	Yes
flow-control-mode	Yes
ftpd	No
ha-cpu	Yes, the standby CPU restarts automatically. Modifying this flag does not require a system restart.
hsecure	Yes
linerate-directed-broadcast	Yes
ipv6-egress-filter	Yes
ipv6-mode	Yes
logging	No
nni-mstp	Yes
reboot	No
rlogind	No
savetostandby	No
spanning-tree-mode	Yes
spbm-config-mode	Yes

Table continues…

CLI flag	Restart
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 RJ–45 jack) to a PC or terminal to monitor and configure the switch. The port uses a RJ–45 connector that operates as data terminal equipment (DTE). Some switches also provide a USB port or micro USB port for serial console interface connectivity. See your hardware documentation for available ports.

The default communication protocol settings for the console port are:

- Baud rate:
  - VSP 4000 Series — 9600
  - VSP 4900 Series — 115200
  - VSP 7200 Series — 9600
  - VSP 7400 Series — 115200
  - VSP 8000 Series — 9600
  - VSP 8600 Series — 115200
  - XA1400 Series — 115200
- 8 data bits
- 1 stop bit
- No parity
- No flow control.

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 can display as console port or 10101.

Client and Server Support

Table 12: Client and Server product support

Feature	Product	Release introduced	Release deprecated
For configuration details, see Administering VOSS.			
File Transfer Protocol (FTP) server and client (IPv4)	VSP 4450 Series	VSP 4000 4.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VSP 8200 4.0	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
File Transfer Protocol (FTP) server and client (IPv6)	VSP 4450 Series	VOSS 4.1	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.1	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 6.2	Not applicable
	XA1400 Series	Not Supported	Not applicable
Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) (IPv4)	VSP 4450 Series	VOSS 4.1	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VSP 8200 4.0	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) (IPv6)	VSP 4450 Series	VOSS 4.1	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.1	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 6.2	Not applicable

Table continues…

Feature	Product	Release introduced	Release deprecated
	XA1400 Series	Not Supported	Not applicable
Remote Login (Rlogin) server/client (IPv4)	VSP 4450 Series	VSP 4000 4.0	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 4.2.1	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VSP 8200 4.0	VOSS 8.2
	VSP 8400 Series	VOSS 4.2	VOSS 8.2
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	VOSS 8.2
Rlogin server (IPv6)	VSP 4450 Series	VOSS 4.1	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 4.2.1	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VOSS 4.1	VOSS 8.2
	VSP 8400 Series	VOSS 4.2	VOSS 8.2
	VSP 8600 Series	VSP 8600 6.2	Not applicable
	XA1400 Series	Not Supported	VOSS 8.2
Rlogin client (IPv6)	VSP 4450 Series	VOSS 7.0	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 7.0	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VOSS 7.0	VOSS 8.2
	VSP 8400 Series	VOSS 7.0	VOSS 8.2
	VSP 8600 Series	VSP 8600 8.0	Not applicable
	XA1400 Series	Not Supported	VOSS 8.2
Remote Shell (RSH) server/client	VSP 4450 Series	VSP 4000 4.0	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 4.2.1	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VSP 8200 4.0	VOSS 8.2
	VSP 8400 Series	VOSS 4.2	VOSS 8.2
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	VOSS 8.2
Secure Copy (SCP)	VSP 4450 Series	VSP 4000 4.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable

Table continues…

Feature	Product	Release introduced	Release deprecated
Note: The switch does not support the WinSCP client.	VSP 7200 Series	VOSS 5.0	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VSP 8200 4.0	Not applicable
	VSP 8400 Series	VOSS 5.0	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
Secure File Transfer Protocol (SFTP) server (IPv4)	VSP 4450 Series	VOSS 4.2	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.2	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
Secure File Transfer Protocol (SFTP) server (IPv6)	VSP 4450 Series	VOSS 4.2	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.2	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 6.2	Not applicable
	XA1400 Series	Not Supported	Not applicable
Telnet server and client (IPv4)	VSP 4450 Series	VSP 4000 4.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VSP 8200 4.0	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
Telnet server and client (IPv6)	VSP 4450 Series	VOSS 4.1	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.1	Not applicable

Table continues…

Feature	Product	Release introduced	Release deprecated
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 6.2	Not applicable
	XA1400 Series	Not Supported	Not applicable
Trivial File Transfer Protocol (TFTP) server and client (IPv4)	VSP 4450 Series	VSP 4000 4.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VSP 8200 4.0	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	Not applicable
TFTP server (IPv6)	VSP 4450 Series	VOSS 4.1	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 4.2.1	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 4.1	Not applicable
	VSP 8400 Series	VOSS 4.2	Not applicable
	VSP 8600 Series	VSP 8600 6.2	Not applicable
	XA1400 Series	Not Supported	Not applicable
TFTP client (IPv6)	VSP 4450 Series	VOSS 7.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 7.0	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 7.0	Not applicable
	VSP 8400 Series	VOSS 7.0	Not applicable
	VSP 8600 Series	VSP 8600 8.0	Not applicable
	XA1400 Series	Not Supported	Not applicable

Table 13: Secure Shell product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Secure Shell (SSH) server (IPv4)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
Secure Shell (SSH) client (IPv4)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
Secure Sockets Layer (SSL) certificate management	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported
SSH server (IPv6)	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	Not Supported
SSH client (IPv6)	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0

Table continues…

Feature	Product	Release introduced
	XA1400 Series	Not Supported
SSH client disable	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
SSH key sizes in multiples of 1024 **Note:** VOSS Releases 6.0 and 6.0.1 do not support this change.	VSP 4450 Series	VOSS 5.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1.2
	VSP 8400 Series	VOSS 5.1.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	Not Supported
SSH rekey	VSP 4450 Series	VOSS 5.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1
	VSP 8400 Series	VOSS 5.1
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.1

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.

Note:

Both FTP and TFTP clients are supported by the switch. The switch does not launch FTP and TFTP clients 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.

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.

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 (fabric or non-fabric mode) 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 in non-fabric mode:

   ```
   boot config flags factorydefaults
   ```

3. Bypass the loading of the switch configuration file and load the factory defaults in fabric mode. This enables Zero Touch Fabric Configuration.

   ```
   boot config flags factorydefaults fabric
   ```

4. 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, check the log file to see if the log file indicates that the factorydefaults setting was enabled, before you investigate other options.

Example

```
Switch:1> enable
```

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

```
Switch:1 (config) # 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 enable TFTP transfers. If you want to use FTP as the transfer mechanism, you need to change the password to a non-null value.

Important:

tftp-debug should be used exclusively to transfer small files less than 1MB in size. Using it for larger files might cause unwanted behavior, such as transfer failure.

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
```

Enable Remote Access Service

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

Before you begin

- When you enable the rlogin flag, you must configure an access policy to specify the user name of who can access the switch. For more information about the access policy commands, see Configuring Security for VOSS.

  Note:

  Rlogin is only supported on VSP 8600 Series.

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

The following table defines parameters for the **boot config flags** command.

Variable	Value
advanced-feature-bandwidth-reservation [low | high] **Note:** Exception: only supported on VSP 7400 Series and XA1480.	Enables the switch to support advanced features by reserving ports as loopback ports. The default is enabled with low level configuration. When disabled, you can use all ports on the switch, but advanced features do not work. The high level means that the switch reserves the maximum bandwidth for the advanced features. The low level means that the switch reserves less bandwidth to support minimum functionality for advanced features.

Table continues…

Variable	Value
	If you change this parameter, you must restart the switch.
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. The boot flag is disabled by default. For information on DvR, see Configuring IPv4 Routing for VOSS.

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 [fabric]	Specifies whether the switch uses the fabric or non-fabric factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the switch restarts. If you change this parameter, you must restart the switch for the change to take effect.
flow-control-mode ✱ **Note:** Exception: not supported on VSP 8600 Series.	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.
ha-cpu ✱ **Note:** Exception: only supported on VSP 8600 Series.	Activates or disables High Availability-CPU (HA-CPU) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable or disable HA mode, the secondary CPU resets automatically to load settings from the saved configuration file.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement

Table continues…

Variable	Value
	• 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-egress-filter **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	Enables IPv6 egress filters. The default is disabled. If you change this parameter, you must restart the switch.
ipv6–mode **Note:** Exception: not supported on VSP 4000 Series, VSP 8600 Series and XA1400 Series.	Enables IPv6 mode on the switch.
linerate-directed-broadcast {true | false} **Note:** Exception: only supported on VSP 4450 Series.	Enables or disables support for IP Directed Broadcast in hardware without requiring CPU intervention. Setting this boot flag will put port 1/46 into loopback mode, making it unusable for external connections, so you need to move any existing connections on this port first. After setting this boot flag, save the configuration, and then restart the switch. The default value is disabled. **Important:** The software cannot be upgraded or downgraded to a software release that does not contain this directed broadcast hardware assist functionality without first disabling this feature and saving the configuration.
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.

Table continues…

Variable	Value
	• The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file. The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
nni-mstp **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	Enables MSTP and VLAN configuration on NNI ports. The default is disabled. **Note:** Spanning Tree is disabled on all NNIs. You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN. You cannot add additional C-VLANs to a brouter port.
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 **Note:** Exception: rlogin and rsh are only supported on VSP 8600 Series.	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby **Note:** Exception: only supported on VSP 8600 Series.	Activates or disables automatic save of the configuration file to the standby CPU. The default value is enabled. If you operate a dual CPU system, it is recommended that you enable this flag for ease of operation.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
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.

Table continues…

Variable	Value
	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.
syslog-rfc5424-format	Controls the format of the syslog output and logging. By default, the switch uses the RFC5424 format. If the RFC based format is disabled, the older format is used.
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 **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	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

Table continues…

Variable	Value
	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 spbmconfig-mode flag, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see Release Notes for VOSS.
vxlan-gw-full-interworking-mode **Note:** Exception: only supported on VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	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 VXLAN Gateway for VOSS.

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

The following table defines parameters for 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.

Configure 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:

Flag support can vary across hardware models.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable boot flags:

   ```
   boot config flags <advanced-feature-bandwidth-reservation [low |
   high] | block-snmp | debug-config [file] | debugmode | dvr-leaf-mode
   | enhancedsecure-mode <jitc|non-jitc> | factorydefaults [fabric] |
   flow-control-mode | ftpd | ha-cpu | hsecure | ipv6-egress-filter |
   ipv6-mode | linerate-directed-broadcast | logging | nni-mstp |
   reboot | rlogind | savetostandby | spanning-tree-mode <mstp|rstp> |
   spbm-config-mode | sshd | syslog-rfc5424-format | telnetd | tftpd |
   trace-logging | urpf-mode | verify-config | vrf-scaling | vxlan-gw-
   full-interworking-mode>
   ```

3. Disable boot flags:

   ```
   no boot config flags <advanced-feature-bandwidth-reservation |
   block-snmp | debug-config [file] | debugmode | enhancedsecure-mode
   <jitc|non-jitc> | dvr-leaf-mode | factorydefaults [fabric] | flow-
   control-mode | ftpd | ha-cpu | hsecure | ipv6-egress-filter | ipv6-
   mode | linerate-directed-broadcast |logging | nni-mstp | reboot |
   rlogind | savetostandby | spanning-tree-mode <mstp|rstp> | spbm-
   config-mode | sshd | syslog-rfc5424-format | 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 <advanced-feature-bandwidth-reservation |
block-snmp | debug-config [file] | debugmode | enhancedsecure-mode
<jitc|non-jitc> | dvr-leaf-mode | factorydefaults [fabric] | flow-
control-mode | ftpd | ha-cpu | hsecure | ipv6-egress-filter | ipv6-
mode | linerate-directed-broadcast | logging | nni-mstp | reboot |
rlogind | savetostandby | spanning-tree-mode <mstp|rstp> | spbm-
config-mode | sshd | syslog-rfc5424-format | 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
```

Activate High Availability mode:

```
Switch:1(config)#boot config flags ha-cpu
Switch:1(config)#save config
```

Variable Definitions

The following table defines parameters for the **boot config flags** command.

Variable	Value
advanced-feature-bandwidth-reservation [low | high] **Note:** Exception: only supported on VSP 7400 Series and XA1480.	Enables the switch to support advanced features by reserving ports as loopback ports. The default is enabled with low level configuration. When disabled, you can use all ports on the switch, but advanced features do not work. The high level means that the switch reserves the maximum bandwidth for the advanced features. The low level means that the switch reserves less bandwidth to support minimum functionality for advanced features. If you change this parameter, you must restart the switch.
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.

Table continues…

Variable	Value
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. The boot flag is disabled by default. For information on DvR, see Configuring IPv4 Routing for VOSS.
enhancedsecure-mode {jitc | non-jitc}	Enables enhanced secure mode in either the JITC or non-JITC sub-modes.

Table continues…

Variable	Value
	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 [fabric]	Specifies whether the switch uses the fabric or non-fabric factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the switch restarts. If you change this parameter, you must restart the switch for the change to take effect.
flow-control-mode **Note:** Exception: not supported on VSP 8600 Series.	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.
ha-cpu **Note:** Exception: only supported on VSP 8600 Series.	Activates or disables High Availability-CPU (HA-CPU) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable or disable HA mode, the secondary CPU resets automatically to load settings from the saved configuration file.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement

Table continues…

Variable	Value
	• 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-egress-filter **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	Enables IPv6 egress filters. The default is disabled. If you change this parameter, you must restart the switch.
ipv6–mode **Note:** Exception: not supported on VSP 4000 Series, VSP 8600 Series and XA1400 Series.	Enables IPv6 mode on the switch.
linerate-directed-broadcast {true | false} **Note:** Exception: only supported on VSP 4450 Series.	Enables or disables support for IP Directed Broadcast in hardware without requiring CPU intervention. Setting this boot flag will put port 1/46 into loopback mode, making it unusable for external connections, so you need to move any existing connections on this port first. After setting this boot flag, save the configuration, and then restart the switch. The default value is disabled. **Important:** The software cannot be upgraded or downgraded to a software release that does not contain this directed broadcast hardware assist functionality without first disabling this feature and saving the configuration.
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.

Table continues…

Variable	Value
	• The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file. The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
nni-mstp **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	Enables MSTP and VLAN configuration on NNI ports. The default is disabled. **Note:** Spanning Tree is disabled on all NNIs. You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN. You cannot add additional C-VLANs to a brouter port.
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 **Note:** Exception: rlogin and rsh are only supported on VSP 8600 Series.	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby **Note:** Exception: only supported on VSP 8600 Series.	Activates or disables automatic save of the configuration file to the standby CPU. The default value is enabled. If you operate a dual CPU system, it is recommended that you enable this flag for ease of operation.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
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.

Table continues…

Variable	Value
	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.
syslog-rfc5424-format	Controls the format of the syslog output and logging. By default, the switch uses the RFC5424 format. If the RFC based format is disabled, the older format is used.
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 **Note:** Exception: not supported on VSP 8600 Series and XA1400 Series.	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

Table continues…

Variable	Value
	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 spbmconfig-mode flag, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see Release Notes for VOSS.
vxlan-gw-full-interworking-mode **Note:** Exception: only supported on VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	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 VXLAN Gateway for VOSS.

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

Note:

This procedure only applies to VSP 8600 Series.

Specify the master CPU to designate which CPU becomes the master after the switch performs a full power cycle. This procedure applies only to hardware with two CPUs.

About this task

Configure the standby-to-master delay to set the number of seconds a standby CPU waits before trying to become the master CPU. The standby-to-master delay applies when two CP modules are booting at the same time. The designated standby CP waits for the configured number of seconds before attempting to assert mastership. Only one CP can be master in a chassis.

⚠ **Caution:**

If you configure the master-to-standby delay to too short a value, the configured standby CP can become a master. If you configure the master-to-standby delay to too long, it can delay the backup CP asserting mastership and continue booting when the designated CP is inserted, but fails booting.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. View the current configuration for the master CPU:

   ```
   show boot config master
   ```

3. Specify the slot of the master CPU:

   ```
   boot config master <1-2>
   ```

4. Save the changed configuration.
5. Configure the number of seconds a standby CPU waits before trying to become the master CPU:

   ```
   boot config delay <0-255>
   ```

6. Save the changed configuration.
7. Restart the switch.

Example

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

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

```
Switch:1(config)# boot config master 2
Switch:1(config)# save config
```

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

```
Switch:1(config)# boot config delay 30
Switch:1(config)# save config
Switch:1(config)# reset
```

Variable Definitions

The following table defines parameters for the **boot config master** command.

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

Reserving Bandwidth for Advanced Features

Use this procedure if you want the switch to support advanced features. When you enable this boot flag, you need to save and reboot with the new configuration.

Before you begin

Product Notice: For VSP 7400 Series, you must ensure your configuration does not include reserved ports before you enable this feature. If the configuration includes reserved ports after you enable this feature and restart the switch, the switch aborts loading the configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable the boot flag:

   ```
   boot config flags advanced-feature-bandwidth-reservation [low |
   high]
   ```

3. Save the configuration, and then reboot the switch.

   Important:

   A change to the advanced-feature-bandwidth-reservation boot flag requires a reboot for the change to take effect.

4. Verify the boot flag configuration:

   ```
   show boot config flags
   ```

5. Verify that the switch reserved the ports as loopback ports. Reserved ports are not visible in the output of the following command:

   Note:

   This step only applies to VSP 7400 Series.

   ```
   show interfaces gigabitEthernet
   ```

Example

Enable this feature to the low level.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#boot config flags advanced-feature-bandwidth-reservation low
   Warning: Please ensure that your configuration does not include ports 1/55-1/56. If
the configuration contains ports 1/55-1/56, loading of config will be aborted.
 Are you sure you want to continue (y/n) ? y
    Warning: Please save the configuration and reboot the switch
             for this to take effect.
             Flag advanced-feature-bandwidth-reservation is changed to enable (low).
```

Displaying Advanced Feature Bandwidth Reservation Ports

Note:

This procedure only applies to VSP 7400 Series.

After you set the **`advanced-feature-bandwidth-reservation`** boot flag and reboot with the new configuration, you can use the following procedure to verify that the switch reserved ports for configuring advanced features such as Fabric Extend, SPB, SMLT, vIST, VXLAN Gateway, Fabric RSPAN (Mirror to I-SID), Application Telemetry, or IS-IS Accept Policies.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display the Advanced Feature Bandwidth Reservation mode and reserved ports:

   `show sys-info`

Example

```
Switch# show sys-info

General Info :

SysDescr     : Switch1 (w.x.y.z)   BoxType: Switch1
SysName      : Switch1
.
.
.

Advanced Feature Bandwidth Reservation:
--------------------------------------------------------------------------------

Reservation Mode : low
Port Usage Info  : 1/31 and 1/32 are not available to use
```

Display 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|master|running-config [verbose]|sio>`

Example

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

```
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
#
#Mon Feb 13 13:32:58 2017 EST
#
boot config flags debug-config file
boot config flags debugmode
boot config flags ftpd
no boot config flags spbm-config-mode
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"
#boot config sio console baud 115200
```

Variable Definitions

The following table defines parameters for 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.
master	Shows the master information.
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.

Configuring serial port devices

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.

Note:

These commands do not appear on all hardware platforms.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. View the current baud rate configuration:

   ```
   show boot config sio
   ```

3. Change the console baud rate:

   ```
   boot config sio console baud <9600–115200> <1-8>|<SF1-SF3>
   ```

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

Example

```
Switch:1>enable
Switch:1#config terminal
Switch:1(config)#show boot config sio
sio console baud 115200 2
sio console baud 115200 5
sio console baud 115200 8
sio console baud 115200 SF1
sio console baud 115200 SF3
```

Configure the baud rate to 9600 for the console port in IOC module slot 2:

```
Switch:1(config)#boot config sio console baud 9600 2
Switch:1(config)#show boot config sio
sio console baud 9600 2
sio console baud 115200 5
sio console baud 115200 8
sio console baud 115200 SF1
sio console baud 115200 SF3
```

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 the following: • 9600 • 19200 • 38400 • 57600

Table continues…

Variable	Value
	• 115200 The default value differs depending on hardware platform: • VSP 4000 Series — 9600 • VSP 4900 Series — 115200 • VSP 7200 Series — 9600 • VSP 7400 Series — 115200 • VSP 8000 Series — 9600 • VSP 8600 Series — 115200 • XA1400 Series — 115200
<1–8> | *<SF1–SF3>* **Note:** Exception: only supported on VSP 8600 Series.	Configures the individual console baud rate for the IOC modules in slots 1 through 8 or the switch fabric (SF) modules in slots SF1 through SF3.

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. Log on as rwa to perform this procedure.
2. To enter User EXEC mode, log on to the switch.
3. Configure the date:

   ```
   clock set <MMddyyyyhhmmss>
   ```

Example

```
Switch:1> enable
Switch:1# clock set 19042014063030
```

Variable definitions

The following table defines parameters for 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

The following table defines parameters for 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.

Configure 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>
   ```

   Note:

   This step only applies to VSP 8600 Series.

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

The following table defines parameters for 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.

Variable	Value
	- 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> ✱ **Note:** Exception: only supported on VSP 8600 Series.	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

The following table defines parameters for 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

The following table defines parameters for 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

The following table defines parameters for the **`clilog`** commands.

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

Configure 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 <1522-9600>
```

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

The following table defines parameters for the **`sys`** command.

Variable	Value
clipId-topology-ip ✱ **Note:** Exception: Only supported on VSP 8600 Series	Configures the topology ip from the available CLIP. *WORD<1-256>*specifies the Circuitless IP interface id.
control tcp-timestamp	Enables or disables TCP Timestamp.
force-msg	Adds forced message control pattern. *WORD<4–4>* Enter force message pattern.
force-topology-ip-flag ✱ **Note:** Exception: Only supported on VSP 8600 Series	Flags set to force choice of topology flag. *enable*
msg-control	Configures system message control feature.
mtu *<1522-9600>*	Configures Jumbo frame support for the data path. The value can be either 1522, 1950 (default), or 9600 bytes.
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).
power	Enables power to specified slot(s).
security-console	Enables the security console.
software	Configures software configuration.
priv-exec-password	Enables authentication for the Privileged EXEC CLI command mode.

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

The following table defines parameters for 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

The following table defines parameters for 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 Mbps Ethernet port that you can use for an Out-of-Band (OOB) management connection to the switch.

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

Note:

Not all hardware platforms include a dedicated, physical management interface. Also, not all speeds are supported on hardware platforms that support a management port. For more information about supported interfaces and speeds, see your hardware documentation.

Management Router VRF

Note:

Management Router is only supported on VSP 8600 Series.

A separate VRF called Management Router (MgmtRouter) is 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.

Note:

IPv6 is not supported on MgmtRouter.

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:

- DNS
- FTP client with the `copy` command
- NTP
- rlogin

  Note:

  Remote login (rlogin) is only supported on the VSP 8600 Series.
- 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.

Note:

IPv6 is not supported on MgmtRouter.

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

Ping test for IPv6:

```
Switch:1(config)#ping 2001:db8::1 vrf vrfRED
2001:db8::1 is alive
```

Traceroute test for IPv4:

```
Switch:1#traceroute 192.0.2.1 vrf MgmtRouter
```

Traceroute test for IPv6:

```
Switch:1#traceroute 2001:db8::1 vrf vrfRED
```

Entity MIB – Physical Table

Table 14: Entity MIB product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Entity MIB - Physical Table	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50
Entity MIB enhancements and integration for the following: • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time object	VSP 4450 Series	VOSS 6.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.1.2
	VSP 8400 Series	VOSS 6.1.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50

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	3 to 8
Fan tray and fan slot	9 to 16
I/O slot	17 to 30
SF Slot	31 to 36
I/O card or module	37 to 50
SF Card	51 to 56
Console port	57
Console port 2	58
Management port	64
Management port 2	65
Power supply	68 to 73
Fan tray	74 to 81
Fan module	82 to 105
Port	192 to 1023
Pluggable Module and Sensor	19201 to 102314

For more information about Entity MIB – Physical Table, see View Physical Entities on page 177.

High Availability-CPU (HA-CPU)

Table 15: High-Availability product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
High Availability-CPU (HA-CPU) for a standalone switch	VSP 4450 Series	Not Applicable
	VSP 4900 Series	Not Applicable
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Applicable
High Availability-CPU (HA-CPU) for Layer 2 with Simplified vIST	VSP 4450 Series	Not Applicable
	VSP 4900 Series	Not Applicable
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	VSP 8600 6.3
	XA1400 Series	Not Applicable
High Availability-CPU (HA-CPU) for Layer 3 with Simplified vIST	VSP 4450 Series	Not Applicable
	VSP 4900 Series	Not Applicable
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	VSP 8600 6.3
	XA1400 Series	Not Applicable

The High Availability-CPU (HA-CPU) framework supports redundancy at the hardware and application levels. The CP software runs on an Input/Output control (IOC) module in both slots 1 and 2, and the HA-CPU feature activates two CPUs simultaneously in master or standby role. These CPUs exchange topology data so that, if a failure occurs, one of the CPUs can take over the operations of the other. You can configure the CPUs to operate in either HA mode or non-HA mode. In HA mode, the two CPUs synchronize configuration, protocol states, and tables. In non-HA mode, the two CPUs do not synchronize.

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

If you switch from one mode to the other, the standby CP restarts in the specified HA mode (hot standby) or non-HA mode (warm standby). This does not impact the Input/Output process and there is no traffic loss on the physical slot of the card.

If a failure occurs and the chassis is configured for either HA mode (hot standby) or non-HA mode (warm standby), the CP software restarts and runs as standby. The system generates a trap to indicate the change from hot-standby mode to warm-standby mode.

Note:

- The HA-CPU feature provides node-level redundancy. Hot standby mode is not supported with fabric functionality, which provides network-level redundancy.

- If your switch is in hot standby mode (ha-cpu boot flag is set to true), you must disable boot config flag to configure SPBM or vIST on the switch. When the switch is in warm standby mode (ha-cpu boot flag is set to false), you must disable SPBM and vIST to move to hot standby mode.
- When you try to switch-over from warm standby mode to hot standby mode using EDM, the system displays the following error message when you enable the boot config flag for ha-cpu:

```
Hot-standby mode cannot be enabled while SPB/VIST features are
still configured.
```

HA mode

In HA mode, also called hot standby, the platform synchronizes the master (primary) CPU information to the standby (secondary) CPU. The platform adds any configuration changes or application table changes to the master CPU by using bulk synchronization or incremental synchronization. Once synchronization is complete, both the CPUs contain the same configuration and application tables information. Application in HA mode support either full HA implementation or partial HA implementation. In full HA implementation, both the configuration and runtime application data tables exist on the master CPU and the standby CPU.

If the master CPU fails, the standby CPU takes over the master responsibility quickly and you do not see an impact on your network. Also, the IOC and SF modules as well as the full HA applications continue to operate and the full HA applications run consistency checks to verify the tables.

The following applications support full HA mode:

Feature	Supported
Layer 1	
Port configuration parameters	Yes
Layer 2	
Media Access Control security (MACsec)	Yes
Multiple Spanning Tree Protocol parameters	Yes
Quality of Service (QoS) parameters	Yes
Rapid Spanning Tree Protocol parameters	Yes
VLAN parameters	Yes
Layer 3	
ARP entries	Yes
Border Gateway Protocol (BGP)	Partial (configuration only)
Dynamic Host Configuration Protocol (DHCP) Relay	Partial (configuration only)
Internet Group Management Protocol (IGMP)	Yes
IPv6	Partial (configuration only)
Access Control Lists	Yes
Open Shortest Path First (OSPF)	Yes
Protocol Independent Multicast (PIM)	Partial (configuration only)

Table continues…

Feature	Supported
Prefix lists and route policies	Yes
Routing Information Protocol	Yes
Router Discovery	Yes
Static and default routes	Yes
Virtual IP (VLANs)	Yes
Virtual Router Redundancy Protocol	Yes
Transport Layer	
Network Load Balancing (NLB)	Yes
Remote Access Dial-In User Services (RADIUS)	Yes
Terminal Access Controller Access-Control System plus (TACACS+)	Partial (configuration only)
UDP forwarding	Yes

Partial HA

A few applications in HA mode have partial HA implementation, where the system synchronizes user configuration data (including interfaces, IPv6 addresses and static routes) from the master CPU to the standby CPU. However, for partial HA implementation, the platform does not synchronize dynamic data learned by protocols. After failure, those applications restart and rebuild their tables, which causes an interruption to traffic that is dependent on a protocol or application with partial HA support.

The following applications support Partial HA:

- Layer 3
  - Border Gateway Protocol (BGP)
  - Dynamic Host Configuration Protocol (DHCP) Relay
  - IPv6
  - Protocol Independent Multicast-Sparse Mode (PIM-SM)
  - Protocol Independent Multicast-Source Specific Mode (PIM-SSM)
- Transport Layer
  - Terminal Access Controller Access Control System plus (TACACS+)

Non-HA mode

In non-HA mode, also called warm standby, the platform does not synchronize the configuration between the master CPU and the standby CPU. When failover happens, the standby CPU switches to master role, and all the IOCs (except the new master CPU) are restarted. The new master CPU loads the configuration when all the cards are ready. These operations cause an interruption to traffic on all ports on the chassis.

Note:

- When there is a switch-over to warm standby mode, only the RWA access level user can log in to the new master CPU console screen.

The remaining users can log in to the CPU console screen only after the master CP module reloads the configuration and displays the new login prompt.

- When the platform switches from standby CPU to master CPU in warm standby mode, the platform always uses the previously-saved primary configuration file to boot the chassis on the switch.
- The runtime config file must be present on the flash drive during the boot-up of both the master CPU and the standby CPU. If the config file that is used by the master CPU for booting is not available on the standby CPU, the standby CPU loads the default config file. You can run the **`save config`** command to synchronize the configuration settings or copy the boot config file from the master CPU to the standby CPU. The standby CPU must be rebooted to load the desired config file.

  When the master CPU is physically removed in warm-standby mode, all cards are rebooted and the standby CPU switches to the master role and loads the saved configuration. If the old master CPU is physically not plugged in during this time, the respective slot configuration is not loaded to memory even though the configuration exists in the config file. When the old master CPU is re-inserted later, the system considers this as a first time insertion and loads the default configuration on the inserted CP card. This is expected behavior in warm-standby mode. To load the configuration for the re-inserted standby CPU, ensure that the **`savetostandby`** boot-flag is set to true after re-inserting the removed CPU, and run the CLI command **`source <config-file>`** on the active CPU.

HA-CPU support in Simplified vIST

HA-CPU in Simplified vIST configurations enables synchronization of data for Layer 2 and Layer 3 applications between the master CPU and standby CPU, to provide hot standby capability.

Power Manager

Table 16: Power Manager product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Power Management	VSP 4450 Series	Not Supported
	VSP 4900 Series	Not Supported
	VSP 7200 Series	Not Supported
	VSP 7400 Series	Not Supported
	VSP 8200 Series	Not Supported
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported

Power Manager identifies the available power in the chassis (called the power budget), and determines if enough power is available to operate the installed components. Power Manager also gives you control over which module slots to supply power to and enables you to prioritize the slots that should shut down first if there isn't enough power available.

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

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

Note:

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

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

For information on configuring Power Manager, see the following:

- If using the CLI, see Configuring power on module slots on page 165 and Configuring slot priority on page 166.
- If using EDM, see Configuring slot priority on page 214.

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 for VOSS.

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 for VOSS.

Auto-Negotiation

Table 17: Auto-Negotiation product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Auto-Negotiation	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1 Switch models: • VSP4900-24S and VSP4900-48P - all fixed ports • VSP4900-12MXU-12XE - all fixed ports, with ports 13 to 24 at 1 Gbps only • VSP4900-24XE - all fixed ports at 1 Gbps only VIM5-4XE at 1 Gbps only and VIM5-4YE at 25 Gbps only
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50

The Auto-Negotiation feature enables the devices to switch between the various operational modes in an ordered fashion and enables you to select a specific operational mode. The Auto-Negotiation feature also provides a parallel detection (called autosensing) function to recognize compatible devices, even if they do not support Auto-Negotiation and helps the device sense the link speed only; not the duplex mode.

You can use the **`show interfaces gigabitEthernet l1-config`** command to see the Auto-Negotiation operational state on a port. The operational state uses the configuration and transceiver type present in the port. If you enable Auto-Negotiation for the port but the transceiver type does not support Auto-Negotiation, the operational state is disabled (false).

10/100/1000 Mbps Port Considerations

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.

Important:

Product-specific considerations for Auto-Negotiation include:

- If Auto-Negotiation is disabled, the following hardware does not support half-duplex:
    - 8424GT ESM
    - 8424XT ESM
    - VSP 7254XTQ
- VIM5-4XE supports Auto-Negotation at 1 Gbps only; Auto-Negotiation at 10 Gbps is not supported.
- VIM5-4X does not support Auto-Negotiation at 1 Gbps.
- Ports 1-24 on VSP4900-24XE and ports 13-24 on VSP4900-12MXU-12XE with 1 Gbps and 10 Gbps supports Auto-Negotiation at 1 Gbps only.

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

Table 18: 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 and cannot shut down misconnected ports. Upper-layer protocols perform these functions.

Note:

The 10 GigabitEthernet (GbE) 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 GbE ports require Auto-Negotiation; Auto-Negotiation is not defined and is non-existent for 10 GbE ports.

For a 10-GbE fiber-based I/O module, you can swap between 1 GbE and 10 GbE operation by simply swapping transceivers. To help with the swap, you can configure Auto-Negotiation when you install a 10 GbE transceiver, even though Auto-Negotiation is not defined for 10 GbE.

You can do this in anticipation of a port changeover from 10 GbE to 1 GbE. In this manner, you can 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.

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.

25 GbE Port Considerations

The 25 GbE ports typically support 25 Gbps, 10 Gbps, and 1 Gbps operational speeds. Auto-Negotiation support varies depending on the pluggable type and speed.

The following table provides a summary of Auto-Negotiation support for 25 Gbps ports.

Table 19: 25 Gbps Port Auto-Negotiation

Transceiver Type	Auto-Negotiation
25 Gbps DAC	Supported VIM5-2Y and VIM5-4Y do not support Auto-Negotiation at 25 Gbps
25 Gbps SR, LR, AOC	Not Supported
10 Gbps	Not Supported
1 Gbps	Not Supported for VSP 7400-48Y

Forward Error Correction (FEC) is a negotiated port attribute for 25 GbE connections that support Auto-Negotiation. For more information, see Forward Error Correction on page 139.

40 GbE Port Considerations

Auto-Negotiation must 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, the best practice is to always enable Auto-Negotiation. Otherwise, there might be link instability or FCS errors.

100 GbE Port Considerations

Ensure that you enable Auto-Negotiation for ports with 100GbCR4 modules plugged in.

Although Auto-Negotiation is mandatory as per the 100GbCR4 standard, and this is the default software configuration, you can disable Auto-Negotiation to connect with older systems that do not support it. The system does not support FEC on 100GbCR4 links with Auto-Negotiation disabled.

For more information about FEC, see Forward Error Correction on page 139.

Auto-Negotiation Advertisements

Auto-Negotiation advertisements 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 Mbps to 10000 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.

Use the **`auto-negotiation-advertisements`** command to configure CANA.

You can use CANA only on 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.

The following platforms (switches and removable modules with RJ-45 Ethernet ports only) support full duplex and half duplex modes for CANA:

Platform	Full duplex	Half duplex
VSP 4450 Series	Yes	Yes
VSP 4900 Series	Yes	Supported at 100Mbps onVSP4900-48P and first 12 ports of VSP4900-12MXU-12XEonly.
VSP 7200 Series	Yes	No
VSP 7400 Series	yes	No
VSP 8200 Series	Yes	No
VSP 8400 Series (includes 8424XT, 8418XTQ, and 8424GT ESMs)	Yes	No

Table continues…

Platform	Full duplex	Half duplex
VSP 8600 Series	Yes	No
XA1400 Series	Yes	Yes Supported on ports 1/1-1/4 only.

SynOptics Network Management Protocol

Table 20: SONMP product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
SONMP	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50

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.

SONMP for the Segmented Management Instance

SONMP and LLDP both advertise the same topology IP address for the Segmented Management Instance management interface. SONMP supports IPv4 advertisement only. If all three management interfaces are configured, the advertised default topology IP priority is management CLIP, then management VLAN, then management OOB. You can change the default topology IP using CLI or EDM. If multiple IPv4 addresses are configured on an OOB or VLAN management interface, the advertised IP priority is static IP address, then DHCP IP address, then link-local IP address.

Channelization

Table 21: Channelization product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Channelization of 40 Gbps ports	VSP 4450 Series	Not Applicable
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0 VSP 7432CQ only
	VSP 8200 Series	VOSS 4.2
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	Not Applicable
Channelization of 100 Gbps ports	VSP 4450 Series	Not Applicable
	VSP 4900 Series	Not Applicable
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	VOSS 8.0 VSP 7432CQ only
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Supported
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	Not Applicable

Use the channelization feature to configure a single port to operate as four individual ports. Channelization can apply to the following port speeds:

- 40 Gbps (Quad Small Form-factor Pluggable) (QSFP+) — when channelized, operates as four 10 Gbps ports
- 100 Gbps (QSFP28) — when channelized, operates as four 25 Gbps ports

Note:

In cases where the hardware supports it, you can insert a 40 Gbps QSFP+ transceiver in a 100 Gbps port, and use the 100 Gbps port as a 40 Gbps port. If you enable channelization on a 100 Gbps port and the switch detects a 40 Gbps QSFP+ transceiver in the port, the port operates as four individual 10 Gbps ports.

If the switch detects a 100 Gbps QSFP28 transceiver and you enable channelization, the port operates as four 25 Gbps ports.

To know if you can use a 100 Gbps port as a 40 Gbps port and support the channelization of that port, see the applicable hardware documentation.

You can use breakout direct attach cables (DAC) or transceivers with fiber breakout cables to connect the channelized ports to other servers, storage, and switches.

By default, the ports are not channelized, which means that the ports operate as one single port at the fully supported speed. You can enable or disable channelization on a port.

For the number of ports on the switch that support channelization, see the applicable hardware documentation.

If the 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 for VOSS.

Note:

When you use channelized ports in an Split Multi-Link Trunking (SMLT) configuration, the channelized ports do not appear properly when you show MLT information for the remote port member if the remote switch runs a release that does not support channelization.

When a port is channelized, use only break out cables (copper or active optical DAC) in it. Using other cables in either a channelized port or a non-channelized port results 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.

Forward Error Correction

Table 22: Forward Error Correction product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Forward Error Correction (FEC) (configurable)	VSP 4450 Series	Not Applicable
	VSP 4900 Series	VOSS 8.1 VIM5-4YE at 25 Gbps
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	Not Supported

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	VOSS 8.0
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	Not Applicable

Forward Error Correction (FEC) is a method of obtaining error control in data transmission over an unreliable or noisy channel in which the source (transmitter) encodes the data in a redundant way by using an error correcting code (ECC). This redundancy enables a destination (receiver) to detect a limited number of errors and correct them without requiring a re-transmission.

FEC is useful where re-transmitting data is either expensive or impossible, for example, when transmitting to multiple receivers in multicast. However, although FEC provides more error control, it introduces a latency in data transmission.

FEC Configuration

You typically configure FEC on a port. The supported options are:

- cl91 (Clause 91 RS-FEC):

  This option supports both the 25 Gbps and 100 Gbps speeds. You can configure this option on ports with either the 100GbSR4 or 100GbCR4 modules plugged in, or on 100 GbE channelized ports operating at 25Gbps speed.

  Note:

  Ensure that you enable Auto-Negotiation for ports with the 100GbCR4 modules plugged in; it is mandatory.

- cl108 (Clause 108 RS-FEC):

  This option also supports both the 25 Gbps and 100 Gbps speeds. It is similar to Clause 91 but provides extra latency.

- cl74 (Clause 74 Firecode R-FEC):

  This option supports only the 25Gbps speed and is used in applications that require reduced latency.

- auto:

  This option automatically configures FEC based on port speed and pluggable module type.

  - For 25 Gbps speeds, FEC CL108 is enabled for all transceiver types.
  - For 100Gbps speeds:
    - FEC is disabled for 100GbE LR4 and ER4 transceivers.
    - FEC CL91 is enabled for all other transceiver types (for example, 100GbE SR4, CR4, AOC, CWDM4, SWDM4).

FEC is not supported on:

- Out-of-band (OOB) management ports.
- 100 GbE ports that are changed to 40 GbE ports by dynamically swapping 100 Gb modules with 40 Gb modules. FEC does not support the 40 Gbps speed.

Important:

- On ports that support FEC configuration, ensure that you configure the same option at both end-points. Otherwise, the link does not come up.
- You must enable FEC to achieve proper functionality when using interconnects such as the 25Gb SR, 25 Gb SR-lite, 25 Gb ESR optics or the 25 Gb AOC and 25 Gb DAC.
- FEC is not required on 100 Gb or 25 Gb long-range optics because these optics do error checking internally.

FEC and Auto-Negotiation

FEC is a negotiated port attribute for 25 Gb and 100 Gb connections that support Auto-Negotiation. If you enable Auto-Negotiation on a port for a supported transceiver type, the switch uses the configured FEC value in the negotiation advertisement. Peers can advertise different values, which means the resulting FEC operational state can be different than the one advertised.

The following table lists the 25 Gb end-point advertisements and the resulting FEC operational state:

Table 23: 25 Gb end-point advertisements

Peer A	Peer B	Result
CL108	CL108	CL108
CL74	CL74	CL74
No FEC	No FEC	No FEC
No FEC	CL108	CL108
No FEC	CL74	CL74
CL74	CL108	CL108

The following table lists the 100 Gb end-point advertisements and the resulting FEC operational state:

Table 24: 100 Gb end-point advertisements

Peer A	Peer B	Result
CL91	CL91	CL91
No FEC	No FEC	CL91 **Note:** Even when both peers advertise no FEC, negotiation results in clause 91 FEC per IEEE standard mandatory setting.
No FEC	CL91	CL91

You can use the **`show interfaces gigabitEthernet config`** command to see the FEC operational state for a port.

IEEE 802.3X Pause Frame Transmit

Table 25: IEEE 802.3X Pause Frame Transmit product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
IEEE 802.3X Pause frame transmit	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.1.50

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

Overview

When congestion occurs on a port, the system can send or receive pause frames, also known as flow control, to temporarily pause the packet flow. The system uses flow control if the rate at which one or more ports receives or sends packets is greater than the rate the switch can process or accept the packets.

The switch can generate 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, 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 26: 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 27: 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.

IOC Module Preconfiguration

Table 28: IOC Module Preconfiguration

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
IOC Module Preconfiguration	VSP 4450 Series	Not supported
	VSP 4900 Series	Not supported
	VSP 4900 Series	Not supported
	VSP 7200 Series	Not supported
	VSP 7400 Series	Not supported
	VSP 8200 Series	Not supported
	VSP 8600 Series	VSP 8600 8.0
	XA1400 Series	Not supported

Using IOC Module Pre-Configuration, you can configure a slot for an IOC Module before you insert the module in the chassis. By specifying the slot and module type, all configuration at the slot or port level become available for that slot. You can issue configuration commands for a specific slot before you insert an IOC Module in that slot.

When you insert the IOC Module that matches the pre-configured module type in the specified slot, all configuration related to that slot is applied, and pre-configuration loads on the IOC Module automatically. However, if the module type of the inserted IOC Module does not match the module type of the IOC Module Pre-Configuration, then the IOC module functionality depends on the following card lock configurations:

- If the card lock option is enabled, the inserted IOC Module is rejected and does not boot up. Only modules that are of same type as the IOC Module Pre-Configuration type for the slot are able to boot up on that slot. The output of the **show-sys-info** command displays the operational status of the inserted module as `down-Mismatch`.
- If the card lock option is disabled, existing configuration is removed on that slot and a new IOC Module is accepted and boots up with default configuration.

When you remove an IOC Module from the chassis, all configuration on that slot is still available because the module was automatically pre-configured on that slot. You can view the configuration for the module by using the **`show sys-info card`** command. You can also change the configuration for an IOC Module that has been removed from the chassis. When you save the configuration, the configuration for all slots is saved regardless of which modules are plugged into the chassis.

Hotswapping IOC Modules

If a preconfigured IOC Module is replaced with a model that does not match the preconfigured IOC Module type and the card lock is enabled, then the IOC Module does not boot up. Either a module of the same type as the preconfigured IOC Module must be reinserted in the slot or the pre-configured IOC Module type must be removed from the configuration.

> **Important:**
> Removing the preconfigured IOC Module type from the configuration also removes the configuration for the slot.

When a new IOC Module is inserted in the slot, the module boots with default configuration. If a module is inserted into a running system and the module type is not configured for the slot, the system automatically creates a preconfiguration with the module type of the IOC Module that was inserted. Then the module boots with default configuration.

Chassis operations configuration using the CLI

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

Enabling the High Availability-CPU (HA-CPU) mode

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the following boot flag:

   ```
   boot config flags ha-cpu
   ```

The configuration file is saved on both the CPUs. After you disable HA mode on the master CPU, the secondary CPU software automatically resets and loads the settings from the previously-saved configuration file.

3. Type `y` after the following prompt appears:

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

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

4. Save the configuration.

Example

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

Enable HA mode:

```
Switch:1(config)#boot config flags ha-cpu
The config files on the Master and Slave will be overwritten with the current active
configuration.
-Layer 2/3 features will be enabled in L2/L3 redundancy mode.
Do you want to continue (y/n)?y
Boot configuration is being saved.
CP-1: Save config to file /intflash/config.cfg successful.
CP-2: Save /intflash/config.cfg to standby successful.
Runtime configuration is being saved.
Resetting Slave CPU from Master CPU.
CP1 [01/07/17 15:21:50.605:UTC] 0x000045e3 00000000 GlobalRouter SNMP INFO Save config
successful.
CP2 [01/07/17 15:22:16.890:UTC] 0x000105e3 00000000 GlobalRouter HW INFO HA-CPU: Table
Sync is complete (Standby CPU)
CP1 [01/07/17 15:22:17.407:UTC] 0x000105c8 00000000 GlobalRouter HW INFO HA-CPU: Table
Sync Completed on Secondary CPU
```

Verify the configuration:

```
Switch:1(config)#show ha-state
Current CPU State : Synchronized State.
Last Event : Table synchronization completed.
Mode : Warm Standby

Card Info :
        Slot#      CardType            Oper   Admin  Power
                                     Status  Status  State
            1        8624XS        up-Master      up     on
            2        8624XS   up-Warmstandby      up     on

Current Boot Config State: master 1
```

Save the configuration:

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

Next steps

Note:

In HA-CPU mode, whenever there is a mismatch of boot config flags between the master CPU and the standby CPU, the standby CPU follows the master CPU. The mismatch could be due to different runtime config files or primary config files at standby CPU. Once the chassis boots up successfully on the switch, ensure that both the CPUs run the same primary config file and the running config file.

Disabling the High Availability-CPU (HA-CPU) Mode

About this task

Perform this procedure to disable HA mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following boot flag command:

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

   The configuration file is saved on both the CPUs. After you enable HA mode on the master CPU, the secondary CPU software automatically synchronizes the configuration from the master CPU.

Example

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

Disable HA mode:

```
Switch:1(config)#no boot config flags ha-cpu
The config files on the Master and Slave will be overwritten with the current active
configuration.
-No longer Layer 2/3 features run in L2/L3 redundancy mode.
Do you want to continue (y/n) ? y
Boot configuration is being saved.
CP-1: Save config to file /intflash/config.cfg successful.
CP-2: Save /intflash/config.cfg to standby successful.
Resetting Slave CPU from Master CPU.
```

Verify the configuration:

```
Switch:1(config)#show ha-state
Current CPU State : Disabled State.
Last Event : No event.
Mode : Warm Standby

Card Info :
        Slot#      CardType             Oper   Admin  Power
                                      Status  Status  State
            1        8624XS        up-Master      up     on
            2        8624XS   up-Warmstandby      up     on

Current Boot Config State: master 1
```

Removing an IOC Module with HA Mode Activated

About this task

Perform this procedure to properly remove the IOC module that is in the master CP slot, when the system operates in HA mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Use the `sys action cpu-switch-over` command to fail over to another CP.
3. Remove the IOC module.

   Important:

   Do not reinsert an IOC module until at least 15 seconds has elapsed, which is long enough for another CP slot to become master.

Example

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

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 <1522-9600>
   ```

Example

```
Switch:1> enable
```

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

Enable jumbo frames to 9600 bytes:

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

Variable Definitions

The following table defines parameters for the **`sys mtu`** command.

Variable	Value
<1522-9600>	Configures the frame size support for the data path. Possible sizes are 1522, 1950 (default), or 9600 bytes.

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

The following table defines parameters for 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 the 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. To enter User EXEC mode, log on to the switch.
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      192.0.2.81     0x000000  0030ab707a00 ChassisType 1          12 Yes HtBt  0/0
1/1      192.0.2.81     0x000000  0050ea268800 ChassisType 2          12 Yes HtBt  1/50
1/42     192.0.2.81     0x000000  070ab307aa00 ChassisType 3          12 Yes HtBt  1/1
2/1      192.0.2.81     0x000000  0030ab57ab00 ChassisType 4          12 Yes HtBt  1/49
2/2      192.0.2.81     0x000000  0030ab307af0 ChassisType 5          12 Yes HtBt  1/50
2/41     192.0.2.81     0x000000  00e0ba327c00 ChassisType 6          12 Yes HtBt  2/1
2/42/1   192.0.2.81     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 29: 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.

Table continues…

Variable	Value
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 for VOSS.

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 the 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
```

Configure an IP Address for the Management Port

Note:

This procedure only applies to VSP 8600 Series.

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).

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 an overlap between in-band and out-of-band networks.

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface mgmtEthernet <mgmt | mgmt2>
   ```

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 192.0.2.24 255.255.255.0
```

Variable Definitions

The following table defines parameters for 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.

The following table defines parameters for the **`ipv6 interface address`** command.

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

Configure Ethernet Ports with Auto-Negotiation

Configure Ethernet ports so they operate optimally for your network conditions.

About this task

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. Otherwise this is not a supported configuration with VSP 7254XSQ.
- 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable Auto-Negotiation:

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

3. Verify the configuration:

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

Example

```
Switch:>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitethernet 1/8
Switch:1(config-if)#auto-negotiate enable
Switch:1(config-if)#show interfaces gigabitEthernet l1-config 1/8
==================================================================================================
                                          Port Config L1
==================================================================================================
PORT     AUTO  OPERATE  CUSTOM AUTO NEGOTIATION    ADMIN       OPERATE     ADMIN         OPERATE
NUM      NEG.  AUTO-NEG ADVERTISEMENTS             DPLX SPD    DPLX SPD    TX-FLW-CTRL   TX-FLW-CTRL
--------------------------------------------------------------------------------------------------
1/8      true  true     Not Configured             full 10000  0           enable       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 varies depending on the platform: • VSP 4000 Series - enabled • VSP 4900 Series - All fixed ports - enabled - VIM5-4X - disabled - VIM5-2Y - disabled • VSP 7400 Series - disabled • VSP 7400 Series - enabled • VSP 8000 Series - enabled • VSP 8600 Series - enabled except for 10G SFP+ ports • XA1400 Series - enabled

Configure Auto-Negotiation Advertisements

Configure local port Auto-Negotiation advertisements to specify the speed and duplex mode for traffic between local ports and remote link partners. Supported speeds and duplex modes vary, depending on your hardware.

Before you begin

You must enable Auto-Negotiation before you perform this procedure.

About this task

Configure local port Auto-Negotiation advertisements.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ✱ **Note:**

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

2. Configure Auto-Negotiation advertisements on one or more ports:

   ```
   auto-negotiation-advertisements {10000-full|2500-full|5000-full|1000-full|100-full|100-half|10-full|10-half}
   ```

   or

   ```
   auto-negotiation-advertisements port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}} {10000-full|2500-full|5000-full|1000-full|100-full|100-half|10-full|10-half}
   ```

3. Verify the configuration:

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

Variable Definitions

The following table defines parameters for the **`auto-negotiation-advertisements`** command.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Specifies the port or ports that you want to configure.
10000-full	Advertises 10000 Mbps full duplex.

Table continues…

Variable	Value
5000-full	Advertises 5000 Mbps full duplex.
2500-full	Advertises 2500 Mbps full duplex.
1000-full	Advertises 1000 Mbps full duplex.
100-full	Advertises 10000 Mbps full duplex.
100-half	Advertises 10000 Mbps half duplex.
10-full	Advertises 10 Mbps full duplex.
10-half	Advertises 10 Mbps half duplex.
none	Configures the Auto-Negotiate value to none.

Configure 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.

Note:

If you enable MACsec on an interface and you send small packet size traffic near line rate, the **`In FlowCtrl`** frame might increment in the output of the **`show interface gigabitEthernet statistics`** command because of the processing overhead caused by adding the MACsec header of 32 bytes. This is part of the expected over-subscription footprint.

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 the 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.

```
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
```

Note:

Flag support can vary across hardware models.

```
Switch:1#show boot config flags
flags advanced-feature-bandwidth-reservation low
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 true
flags ha-cpu true
flags hsecure false
flags ipv6-egress-filter true
flags ipv6-mode false
flags linerate-directed-broadcast false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags savetostandby true
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags syslog-rfc5424-format true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode true
flags verify-config true
flags vrf-scaling true
flags vxlan-gw-full-interworking-mode false
```

```
Switch:1(config-if)#show interfaces gigabitEthernet l1-config 1/10
====================================================================================================
                                           Port Config L1
====================================================================================================
PORT     AUTO  OPERATE  CUSTOM AUTO NEGOTIATION    ADMIN       OPERATE     ADMIN          OPERATE
NUM      NEG.  AUTO-NEG ADVERTISEMENTS              DPLX SPD    DPLX SPD    TX-FLW-CTRL    TX-FLW-CTRL
----------------------------------------------------------------------------------------------------
1/10     true  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

The following table defines parameters for 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 the 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 the 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:

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

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

```
enable
```

```
configure terminal
```

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

Note:

If the 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

The following table defines parameters for 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 the platform supports channelization and the port is

Variable	Value
	channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring FEC on a port

About this task

Use this procedure to configure Forward Error Correction (FEC) on supported ports.

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

2. **(Optional)** Specify the port or ports to configure for FEC:

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

3. Configure FEC on a port:

   `fec {auto | cl108 | cl74 | cl91}`

4. Verify the configuration:

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

Example

Configure Clause 108 FEC on a 25 Gbps port 1/1 :

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitethernet 1/1
Switch:1(config-if)#fec cl108
```

Verify the configuration when a 25 Gbps optic is present:

```
Switch:1(config-if)#show interfaces gigabitEthernet config 1/1
============================================================================================
                                   Port Config
============================================================================================
PORT                          DIFF-SERV    QOS   MLT   VENDOR
NUM      TYPE                 EN    TYPE   LVL   ID    NAME
--------------------------------------------------------------------------------------------
1/1      25GbCX               true  core   1     0     Extreme
============================================================================================
                                  Port Config
==========================================================================================

PORT   ADMIN   OPERATE AUTO     ACCESS-SERV  RMON     FLEX-UNI  ADMIN  APPLICABLE  OPERATE
NUM    ROUTING ROUTING RECOVER  EN                              FEC    FEC         FEC
------------------------------------------------------------------------------------------
1/1   Enable   Disable Disable false         Disable  Disable   Auto  CL108      CL108
```

Verify the configuration when a 10 Gb optic is present in the 25 Gb port:

```
Switch:1(config-if)#show interfaces gigabitEthernet config 1/1
==========================================================================================
                                  Port Config
==========================================================================================
PORT                         DIFF-SERV    QOS   MLT    VENDOR
NUM      TYPE                EN     TYPE  LVL   ID     NAME
------------------------------------------------------------------------------------------
1/1      10GbSR              true   core  1     0      Extreme

PORT   ADMIN   OPERATE AUTO     ACCESS-SERV  RMON     FLEX-UNI  ADMIN  APPLICABLE        OPERATE
NUM    ROUTING ROUTING RECOVER  EN                              FEC    FEC               FEC
------------------------------------------------------------------------------------------------
1/1   Enable   Disable Disable  false        Disable  Disable   Auto  Not Applicable     Off
```

Variable Definitions

The following table defines parameters for the **fec** command.

Variable	Value
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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
{auto | cl108 | cl74 | cl91}	Configures one of the following options for FEC on the port: • auto • Clause 91 • Clause 108 • Clause 74 **Note:** On a 100 GbE port, only the Clause 91 and Clause 108 options are supported. On 100 GbE channelized ports (operating at 25 Gbps speed), you can configure Clause 108 for extra latency or Clause 74 for reduced latency. Configuration of FEC is not supported on a management port or on 100 GbE ports operating at 40 Gbps speed.

Table continues…

Variable	Value
	Important: On ports that support FEC, always configure the same option on both end-points. Otherwise, the link does not come up.

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 532.

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
```

Configuring power on module slots

About this task

Use this procedure to control whether or not to supply power to specific slots that contain either switch fabric modules or input/output modules. By default, power is available to all slots.

After enabling power to specific input/output module slots, you can also configure the priority in which they are powered on. For more information, see Configuring Slot Priority on page 166.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable power to one or more slots:

   ```
   sys power slot <1-4 | 1-8 | SF1-SF3>
   ```

3. Disable power to one or more slots:

   ```
   no sys power slot <1-4 | 1-8 | SF1-SF3>
   ```

Example

```
Switch:1>enable
```

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

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 3 and 5:

```
Switch:1(config)#sys power slot 3,5
```

Disable power to Slots 3 and 5:

```
Switch:1(config)#no sys power slot 3,5
```

Variable Definitions

The following table defines parameters for the **sys power slot** command.

Variable	Value
<1–4 | 1–8 | SF1–SF3>	Identifies the slot to provide power in one of the following formats: a single slot (1), a range of slots (1–3), or a series of slots (1,2,4). The default is to provide power to all slots.

Variable	Value
	Use the no operator to disable power to a slot. Use the default operator to enable power to a slot. Different hardware platforms support different slot ranges. Use the CLI Help to see the available range.

Configuring Slot Priority

Note:

This procedure only applies to VSP 8600 Series.

About this task

Configure slot priority to specify which slots you want to shut down if there is insufficient power available in the chassis. By default, power is available to all slots, and the slots have the following priority:

- Slots 1, 2, SF1, SF2, and SF3 must always be *Critical* so you cannot configure them.
- Slots 3-8 are *High* by default, but you can configure any of them to *Low*.

Note:

Power is always supplied to critical slots first which are the CP modules, SF modules, and fan trays.

The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first) and interface slots shut down before CP, SF modules, and fan tray slots.

For example, if slot 3 has a `low` priority and slots 4 and 5 have a `high` priority, the slot shutdown priority is as follows: 4, 5, 3. Slot 3 has the lowest priority because it was configured as `low` so it would be shut down first. Slots 4 and 5 have the same priority, but slot 5 shuts down before slot 4 because slot 4 has a higher slot number.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure slot priority:

   ```
   sys power slot-priority <3–8> {high|low}
   ```

Example

```
Switch:1>enable
```

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

Configure slot priority to determine that slot 3 has a low priority if insufficient power is available for all modules:

```
Switch:1(config)#sys power slot-priority 3 low
```

Variable Definitions

The following table defines parameters for the **`sys power slot-priority`** command.

Variable	Value
<3–8>	Identifies the module slot.
high | low	Specifies whether the module should have a high or low priority setting if there is insufficient power available for all modules. The default is high.

Enable the Locator LED

✱ **Note:**

This procedure only applies to VSP 4900 Series.

About this task

Perform this procedure to turn the system Locator LED on to provide a visual identification of a specific switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable the system Locator LED:

   ```
   sys locator-led
   ```

3. Display the system Locator LED status:

   ```
   show sys locator-led
   ```

Enable or disable 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 Series switch.

The USB FLASH drive on all models of the VSP 4850 Series (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 Series 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
   ```

Configure Port Speed

About this task

Manually configure the port speed.

Important:

If Auto-Negotiation is disabled and you change the speed on a port that results in a configuration mismatch in speed between two ports, VSP 4450 Series and VSP 4900 Series switches may show an incorrect operational status of "up" for the mismatched ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

Note:

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

2. Configure the speed for one or more ports:

```
speed {10|100|1000|10000|2500|25000|5000}
```

or

```
speed port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}] {10|
100|1000|10000|2500|25000|5000}
```

Variable Definitions

The following table defines parameters for the **speed** command.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Specifies the port or ports that you want to configure.
10	Configures the port speed to 10 Mbps.
100	Configures the port speed to 100 Mbps.
1000	Configures the port speed to 1 Gbps.
10000	Configures the port speed to 10 Gbps.
2500	Configures the port speed to 2.5 Gbps.
25000	Configures the port speed to 25 Gbps.
5000	Configures the port speed to 5 Gbps.

Configure Ports Speeds for All VIM Ports

Note:

This procedure only applies to VSP 4900 Series.

Configure all of the ports on an installed Versatile Interface Module (VIM) to operate at the same speed.

Note:

Some VIMs must operate with all ports at the same speed, while others can operate with ports at different speeds. For more information, see Release Notes for VOSS. The **sys vim-speed** command is supported only on VIMs that must operate with all ports at the same speed. An error message displays if you run the command on an unsupported VIM.

Before you begin

Install the VIM before performing this procedure.

About this task

Use this procedure to configure the speed of all ports in a multi-port VIM to operate at either 10 Gbps or 25 Gbps.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the speed for all of the VIM ports:

   ```
   sys vim-speed {10000 | 25000}
   ```

Variable Definitions

The following table defines parameters for the **sys vim-speed** command.

Variable	Value
10000 | 25000	Configures all ports in a multi-port VIM to operate at either 10 Gbps or 25 Gbps. The default is 25 Gbps.

Display Ports Speeds for All VIM Ports

Note:

This procedure only applies to VSP 4900 Series.

Display the configured speed on all VIM ports.

Note:

Some VIMs must operate with all ports at the same speed, while others can operate with ports at different speeds. For more information, see Release Notes for VOSS. The **show sys vim-speed** command is supported only on VIMs that must operate with all ports at the same speed. An error message displays if you run the command with an unsupported VIM installed.

Before you begin

Install the VIM before performing this procedure.

About this task

Use this procedure to display the configured speed of all ports in a multi-port VIM.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display the speed for all of the VIM ports:

```
show sys vim-speed
```

Prepare a slot for IOC Module Preconfiguration using CLI

About this task

Use this procedure to designate a slot in the switch for IOC module preconfiguration. You can designate a slot for only one module type at a time.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

3. Designate a slot for IOC module preconfiguration:

   ```
   preconfig slot <1-8> WORD<1-20> [lock]
   ```

4. Verify IOC module preconfiguration:

   ```
   show sys-info card
   ```

Example

The following examples prepare a slot for IOC module preconfiguration:

Prepare a slot for IOC module preconfiguration, with card lock enabled on the slot.

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

Switch:1(config)#preconfig slot 5 8624XT lock
```

Verify the configuration:

```
Switch:1(config)#show sys-info card

Card Info :
  Slot 5 :

        CardType           : 8624XT
        CardDescription    : 8624XT
        CardSerial#        : SDNI86XSD282
        CardPart#          : EC8604002-E6
        CardAssemblyDate   : 20161125
        CardHWRevision     : D2
        CardHWConfig       : 0
        AdminStatus        : up
        OperStatus         : up
        PowerStatus        : on
        Preconfigured      : yes
        Preconfig CardType: 8624XT
        Preconfig Lock     : yes
```

If card lock is enabled on the slot, and the module type of the inserted IOC module does not match the preconfigured IOC module type (for example, if the inserted module is type 8624XT but the preconfigured module type is 8624XS), then the operational status of the inserted IOC module displays as `down-Mismatch`.

```
Switch:1(config)show sys-info card

Card Info :
  Slot 5 :

        CardType           : 8624XS
        CardDescription    : 8624XS
        CardSerial#        : SDNI86XSD282
        CardPart#          : EC8604002-E6
        CardAssemblyDate   : 20161125
        CardHWRevision     : D2
        CardHWConfig       : 0
        AdminStatus        : down
        OperStatus         : down-Mismatch
        PowerStatus        : down
        Preconfigured      : yes
        Preconfig CardType: 8624XT
        Preconfig Lock     : yes
```

Prepare another slot for IOC module preconfiguration, with no card lock enabled on the slot.

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

Switch:1(config)#preconfig slot 6 8624XS
```

Verify the configuration:

```
Switch:1(config)show sys-info card

Card Info :
  Slot 6 :

        CardType           : 8624XS
        CardDescription    : 8624XS
        CardSerial#        : SDNI86XSD282
        CardPart#          : EC8604002-E6
        CardAssemblyDate   : 20161125
        CardHWRevision     : D2
        CardHWConfig       : 0
        AdminStatus        : up
        OperStatus         : up
        PowerStatus        : on
        Preconfigured      : yes
        Preconfig CardType: 8624XS
        Preconfig Lock     : no
```

If card lock is disabled on the slot, and the IOC module type of the inserted card does not match the preconfigured module type, the existing configuration is deleted and the slot is automatically preconfigured with the module type of the inserted IOC module. The inserted module then boots up with default configuration.

In the following example, when the 8624XT module is inserted in a slot preconfigured for the 8624XS, the pre-configuration for the 8624XS is deleted because it is not locked. The slot is then automatically preconfigured for 8624XT when the IOC module is physically inserted in that slot.

```
Switch:1(config)show sys-info card

Card Info :
  Slot 6 :

        CardType          : 8624XT
        CardDescription   : 8624XT
        CardSerial#       : SDNI86XSD282
        CardPart#         : EC8604002-E6
        CardAssemblyDate  : 20161125
        CardHWRevision    : D2
        CardHWConfig      : 0
        AdminStatus       : up
        OperStatus        : up
        PowerStatus       : on
        Preconfigured     : yes
        Preconfig CardType: 8624XT
        Preconfig Lock    : no
```

Variable Definitions

The following table defines parameters for the **`preconfig slot`** command.

Variable	Value
`<1-8>`	Specifies the slot number designated for pre-configuration.
`WORD <1-20>`	Specifies the card type that can be assigned to the pre-configured slot.
`lock`	Specifies that the IO card will be locked to the pre-configured slot. Only the IO card that matches the card type assigned to the pre-configured slot will operate.

Chassis operations configuration using EDM

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

Edit System Information

About this task

Edit system identification information, configuration file information, and perform system actions.

Procedure

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

3. Click the **System** tab.
4. Enter or edit the information as required.
5. 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.
VirtualIpAddr	Configures the virtual IP address that the primary CPU advertises and stores in the switch configuration file.
VirtualNetMask	Configures the net mask of the virtual management IP address.
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

Table continues…

Name	Description
LicenseFileName + **Note:** Exception: only supported on the XA1400 Series and the VSP 8600 Series.	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
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
ActionGroup4	Can be the following action: • softReset—resets the device without running power-on tests • cpuSwitchOver—switches over to the other CPU • softResetCoreDump —reset with coredump
Result	Displays a message after you click **Apply**.
LocatorLED **Note:** Exception: only supported on VSP 4900 Series.	Configures the system Locator LED on or off. The default is off.

Edit 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 **Configuration** > **Edit**.
3. Select **Chassis**.
4. Select the **Chassis** tab.
5. Edit the necessary options.
6. Select **Apply**.

Chassis Field Descriptions

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

Name	Description
Type	Specifies the chassis type.
ModelName This parameter does not appear on all platforms.	Specifies the chassis model name.
BrandName This parameter does not appear on all platforms.	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 Series: 1 slot • VSP 4900 Series: 2 slots • VSP 7200 Series: 2 slots • VSP 7400 Series: 1 slot • VSP 8200 Series: 1 slot • VSP 8400 Series: 4 slots • VSP 8600 Series: 8 slots • XA1400 Series: 1 slot
NumPorts	Specifies the number of ports currently installed in the chassis.
BaseMacAddr	Specifies the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
MacAddrCapacity	Specifies the 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.

Table continues…

Name	Description
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 on all platforms.	Specifies the amount of power the CPU uses.
PowerAvailable This parameter does not appear on all platforms.	Specifies the amount of power available to the CPU.

View Physical Entities

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

Procedure

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

Physical Entities Field Descriptions

The following table defines the use the Physical Entities tab.

Name	Description
Index	Indicates the index of the entry.

Table continues…

Name	Description
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. 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

Table continues…

Name	Description
	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 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.

Table continues…

Name	Description
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.

View Entity Aliases

About this task

Perform this procedure to view the entity aliases on the switch.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Entity**.
3. Click the **Alias** tab.

Alias Field Descriptions

Use the following table to use the Alias tab.

Name	Description
Index	The index of the entry
LogicalIndexOrZero	The index of the entry. The value of this object identifies the logical entity that defines the naming scope for the associated instance of the Mapping Identifier object. This is always 0.
MappingIdentifier	The value of this object identifies a particular conceptual row associated with the indicated Physical Index and Logical Index pair. Because only physical ports are modeled in this table, only entries that represent interfaces or ports are allowed. If an ifEntry exists on behalf of a particular physical port, then this object should identify the associated ifEntry. This is the OID of ifIndex.Port.

Viewing Entity Child Indexes

About this task

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Entity**.
3. Click the **Child Index** tab.

Child Index field descriptions

Use the following table to use the Child Index tab.

Name	Description
Index	Indicates the index of the entry.
ChildIndex	The index of the entry. The value of Physical Index for the contained physical entity.

Configure 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 **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. Select the system flags you want to activate.
5. Clear the system flags you want to deactivate.
6. Click **Apply**.

   Important:

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

System Flags Field Descriptions

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

Name	Description
EnableAccessPolicy	Activates access policies. The default is disabled.
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	Enables the system to send the authentication success trap, rcnAuthenticationSuccess. The default is disabled.
MrouteStrLimit	Enable or disable Mroute stream limit in system. The default is disabled.
DataPathFaultShutdownEnable	Enable or disable data path fault shutdown. The default is enabled.
PingTracerouteContextType ✱ **Note:** Exception: not supported on VSP 8600 Series.	Configures the default context for executing ping commands and traceroute commands. The default is grt.
UdpSrcByVirtualIpEnable	Enables or disables virtual IP as the User Datagram Protocol (UDP) source. The default is disabled.
ForceTopologyIpFlagEnable	Activates or disables the flag that configures the CLIP ID as the topology IP. Values are true or false. The default is disabled.
CircuitlessIpId	Uses the CLIP ID as the topology IP. Enter a value from 1–256.
HaCpu	Activates or disables the CPU High Availability feature. If you enable or disable High Availability mode, the secondary CPU resets automatically to load settings from the saved configuration file. The default is enabled.
MasterCPUSlot	Specifies the slot number, either 1 or 2, for the master CPU. The default value is 1.
EnableSavetoStandby	Enables or disables automatic save of the configuration file to the standby CPU. The default value is enabled.
HaCpuState	Indicates the CPU High Availability state. • initialization—Indicates the CPU is in this state. • oneWayActive—Specifies modules that need to synchronize register with the framework (either locally or a message received from a remote CPU).

Table continues…

Name	Description
	• twoWayActive—Specifies modules that need to synchronize register with the framework (either locally or a message received from a remote CPU). • synchronized—Specifies table-based synchronization is complete on the current CPU. • remoteIncompatible—Specifies CPU framework version is incompatible with the remote CPU. • error—Specifies if an invalid event is generated in a specific state the CPU enters Error state. • disabled—Specifies High Availability is not activated. • peerNotConnected—Specifies no established peer connection. • peerConnected—Specifies peer connection is established. • lostPeerConnection—Specifies a lost connection to peer or standby CPU. • notSynchronized—Specifies table-based synchronization is not complete.
HaEvent	Indicates the High Availability event status. • restart—Causes the state machine to restart. • systemRegistrationDone—Causes the CPU to transfer to One Way or Two Way Active state. • tableSynchronizationDone—Causes the CPU to transfer to synchronized state. • versionIncompatible—Causes the CPU to go to remote incompatible state • noEvent—Means no event occurred to date.
StandbyCpu	Indicates the state of the standby CPU.

Configure Channelization

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

Important:

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 for VOSS.

Procedure

1. In the Device Physical View tab, select a port that supports channelization.
2. In the navigation pane, expand **Configuration** > **Edit** > **Port**.
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 **Configuration** > **Edit** > **Port**.
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**.

Configure basic port parameters

Configure options for port operations.

About this task

If you select more than one port, the format of the tab changes to a table-based tab.

Note:

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. Otherwise this is not a supported configuration with VSP 7254XSQ.

- 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 one or more ports.
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 Extreme Networks 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.

Table continues…

Name	Description
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 ✳ **Note:** Exception: only supported on VSP 7200 Series.	Shows the port license status.
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. The default varies depending on the platform: • VSP 4000 Series - Enabled • VSP 4900 Series - Enabled • VSP 7200 Series - Disabled • VSP 7400 Series - Enabled • VSP 8200 Series - Enabled • VSP 8400 Series - Enabled • VSP 8600 Series - Enabled (except 10 Gbps SFP+ ports) • XA1400 Series - Enabled (except 10 Gbps SFP+ ports)
AutoNegAd	Specifies the port speed and duplex abilities to advertise during link negotiation. Supported speeds and duplex modes vary, depending on your hardware. 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).

Table continues…

Name	Description
	Any change to this configuration restarts the auto-negotiation process, which has the same effect as physically unplugging and reattaching the cable attached to the port. If you select **default**, all capabilities supported by the hardware are advertised.
AdminDuplex	Configures the administrative duplex setting for the port.
OperDuplex	Indicates the operational duplex setting for the port.
AdminSpeed	Configures the administrative speed for the port. **Important:** If Auto-Negotiation is disabled and you change the administrative speed on a port that results in a configuration mismatch in speed between two ports, VSP 4450 Series and VSP 4900 Series switches may show an incorrect operational status of "up" for the mismatched ports.
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).
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.

Table continues…

Name	Description
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
FlexUniEnable	Enables Flex UNI on the port. The default is disabled.
IngressRateLimit **Note:** Exception: only supported on VSP 4900 Series, VSP 7200 Series, VSP 8200 Series, VSP 8400 Series, and XA1400 Series.	Limits the traffic rate accepted by the specified ingress port.
IngressRatePeak	Configures the peak rate in Kbps. The default is 0.
IngressRateSvc	Configures the service rate in Kbps. The default is 0.
EgressRateLimitState	Enables or disables egress port-based shaping to bind the maximum rate at which traffic leaves the port. The default is disabled.
EgressRateLimit **Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series.	Specifies the egress rate limit in Kbps. Different hardware platforms support different egress rate limits, depending on the port with the highest speed available on the platform. You cannot configure the egress shaper rate to exceed the port capability. If you configure this value to 0, shaping is disabled on the port.
TxFlowControl **Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, VSP 8400 Series, and XA1400 Series.	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.
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 of 0 or 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.

Table continues…

Name	Description
ForwardErrorCorrection	Configures one of the following options for Forward Error Correction (FEC) on the port: • CL 91 • CL 108 • CL 74 • disable • auto The disable option disables this configuration on the port.
ForwardErrorCorrectionApplicability	Displays whether FEC is applicable on the interface.
OperAutoNegotiate	Shows the operational state of Auto-Negotiation.
OperForwardErrorCorrection	Shows the negotiated operational FEC clause. If the value is off, the port supports FEC and is up but not configured for FEC. If the value is notApplicable, the port does not support FEC. If the value is unknown, the port supports FEC but is down.
IsPortShared	Indicates whether the port is combo or not. • portShared—Combo port. • portNotShared—Not a combo port.
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.
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 the result of the selected action. The default is none.

Configure Basic Parameters on an Extreme Integrated Application Hosting Port

About this task

Perform this procedure to configure basic parameters on Extreme Integrated Application Hosting (IAH) ports, for example, auto negotiation, QoS level, and remote monitoring.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Insight Port**.
2. Select the IAH port you want to configure.
3. Select the **Interface** tab.
4. In the **Name** field, type a name for the IAH port.
5. Configure the fields as required.
6. Select **Apply**.

Interface Field Descriptions

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

Name	Description
Index	Specifies the index of the Extreme Integrated Application Hosting (IAH) port, written in the slot/ port[/sub-port] format.
Name	Specifies the name of the IAH port.
Descr	Specifies the information about the interface.
Type	Specifies the type of connector plugged in the IAH port.
Mtu	Specifies 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	Specifies the physical address of the IAH 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 (like a serial line), this object should contain an octet string of zero length.
VendorDescr	Specifies the vendor of the connector plugged in the IAH port.

Table continues…

Name	Description
DisplayFormat	Specifies the slot and port numbers (slot/port).
AdminStatus	Specifies the operational status of the IAH port. The testing state indicates that no operational packets can be passed.
OperStatus	Specifies the current status of the IAH port. The testing state indicates that no operational packets can be passed.
LicenseControlStatus	Specifies the IAH port license status.
ShutdownReason	Specifies the reason for the IAH port state change.
LastChange	Specifies the timestamp of the last change.
LinkTrap	Enables or disables link trapping. The default is enabled.
AutoNegotiate	Enables or disables auto-negotiation for the IAH port. The default is true (enabled).
AutoNegAd	Specifies the port speed and duplex abilities to be advertised during link negotiation. The abilities specified in this object are only used when auto-negotiation is enabled on the IAH port. If all bits in this object are disabled, and auto-negotiation is enabled on the IAH port, then the physical link process on the IAH port will be disabled (if hardware supports this ability). Any change in the value of this bit map will force the switch to restart the auto-negotiation process. 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. By default, all capabilities supported by the hardware are enabled.
AdminDuplex	Specifies the administrative duplex setting for the IAH port.
OperDuplex	Specifies the operational duplex setting for the IAH port.
AdminSpeed	Specifies the administrative speed for the IAH port.
OperSpeed	Specifies the operational speed for the IAH port.
QoSLevel	Specifies the Quality of Service (QoS) level for the IAH port. The default is level1.
DiffServ	Enables the Differentiated Service feature for the IAH port. The default is enabled.

Table continues…

Name	Description
Layer3Trust	Specifies 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 or disabled. The default is disabled.
MltId	Specifies the MLT ID associated with the IAH port. The default is 0.
Locked	Specifies if the IAH port is locked. The default is false.
UnknownMacDiscard	Enables the functionality to discard packets with an unknown source MAC address, and prevents the other IAH port from sending packets with the same MAC address as the destination MAC address. The default is disabled.
DirectBroadcastEnable	Specifies if the IAH port forwards direct broadcast traffic.
OperRouting	Specifies the routing status of the IAH port. The default is disabled.
HighSecureEnable	Enables or disables the high secure feature for the IAH port. The default is disabled.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the IAH port. The default is disabled.
FlexUniEnable	Enables or disables Flex UNI on the IAH port. The default is disabled.
EgressRateLimitState	Enables or disables egress port-based shaping to bind the maximum rate at which traffic leaves the IAH port. The default is disabled.
EgressRateLimit	Specifies the egress rate limit in Kbps. Different hardware platforms provide different port speeds. The default is 0.
TxFlowControl	Specifies if the IAH port is sending pause frames. The default is disabled. **Note:** You must enable the flow control feature globally.
TxFlowControlOperState	Specifies the operational state of flow control.
BpduGuardTimerCount	Specifies the duration since when the IAH port is disabled. When the BpduGuardTimerCount reaches the BpduGuardTimeout value, the IAH port is enabled.

Table continues…

Name	Description
BpduGuardTimeout	Specifies the time (in seconds) for the IAH port-state recovery. After the IAH port is disabled by the BPDU guard, the IAH port remains in the disabled state until this timer expires. The default is 120 seconds. If you configure the value to 0, the expiry is infinity.
BpduGuardAdminEnabled	Enables or disables BPDU Guard on the IAH port. The default is disabled.
ForwardErrorCorrection	Configures one of the following options for Forward Error Correction (FEC) on the IAH port: • CL 91 • CL 108 • CL 74 • disable • auto The disable option disables this configuration on the port.
ForwardErrorCorrectionApplicability	Displays whether FEC is applicable on the interface.
OperAutoNegotiate	Shows the operational state of Auto-Negotiation.
OperForwardErrorCorrection	Shows the negotiated operational FEC clause. If the value is off, the port supports FEC and is up but not configured for FEC. If the value is notApplicable, the port does not support FEC. If the value is unknown, the port supports FEC but is down.
Action	Specifies the following actions on the IAH port: • none - no action. • 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. • clearLoopDetectAlarm - clears the loop detection alarm on the IAH port. The default is none.
Result	Specifies the result of the selected action. The default is none.

Configure 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 **Configuration** > **Edit**.
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 **Configuration** > **Edit** > **Port**.
10. Click **General**.
11. Click the **Interface** tab.
12. For TxFlowControl, select **enable** to enable the interface to generate pause frames.
13. Click **Apply**.

View 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 **Configuration** > **Edit**.
3. Select **Chassis**.
4. Select the **Boot Config** tab.

Boot Config Field Descriptions

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

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time image.
PrimaryConfigSource	Specifies the primary configuration source.
PrimaryBackupConfigSource	Specifies the backup configuration source to use if the primary does not exist.
EnableFactoryDefaultsMode	Specifies whether the switch uses the factory default settings at startup. • **false**: The node does not use factory default settings at startup. • **fabric**: The node uses the factory default fabric mode settings at startup. Zero Touch Fabric Configuration is enabled. • **noFabric**: The node uses the factory default mode settings at startup. The default value is false. This flag is automatically reset to the default setting after the switch restarts. If you change this parameter, you must restart the switch for the change to take effect.
EnableDebugMode	Enabling the debugmode allows a 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. The default value 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 value is disabled.
EnableRloginServer ✱ **Note:** Exception: only supported on VSP 8600 Series.	Activates or disables the rlogin and rsh server. The default value is disabled.

Table continues…

Name	Description
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 ✱ **Note:** Exception: not supported on VSP 4000 Series or XA1400 Series .	Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. This flag is disabled by default.
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 ✱ **Note:** Exception: only supported on VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	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. In Base Interworking Mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments.
EnableFlowControlMode ✱ **Note:** Exception: not supported on VSP 8600 Series.	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

Table continues…

Name	Description
	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.
AdvancedFeatureBwReservation **Note:** Exception: only supported on VSP 7400 Series and XA1480. Exception: only low level supported on XA1480.	Enables the switch to support advanced features. The default is enabled with low level configuration. The high level means that the switch reserves the maximum bandwidth for the advanced features. The low level means that the switch reserves less bandwidth to support minimum functionality for advanced features. If you change this parameter, you must restart the switch.
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 for VOSS.
EnableSyslogRfc5424Format	Enables or disables the RFC 5424 syslog format. The default is enabled. If the pre-existing configuration file is for a release prior to this enhancement, then the flag is disabled automatically.
NniMstp	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.
EnableIpv6EgressFilterMode	Enables IPv6 egress filters. The default is disabled.

Table continues…

Name	Description
	If you change this parameter, you must restart the switch.
MasterCPUSlot ✱ **Note:** Exception: only supported on VSP 8600 Series.	Specifies the slot number, either 1 or 2, for the master CPU. The default value is 1.
EnableHaCpu ✱ **Note:** Exception: only supported on VSP 8600 Series.	Enables or disables the CPU High Availability feature. If you enable or disable HA mode, the secondary CPU automatically resets to load settings from the previously-saved configuration file. The default is enabled.
EnableSavetoStandby ✱ **Note:** Exception: only supported on VSP 8600 Series.	Enables or disables automatic save of the configuration file to the standby CPU. The default value is enabled.
Slot	Specifies the slot number.
TftpHash	Enables TFTP hashing.
TftpRetransmit	Set TFTP retransmit timeout counter.
TftpTimeout	Set TFTP timeout counter.
User	Configure host user.
Password	Configure host password.

Configure 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 **Configuration** > **Edit** > **Chassis**.
2. Select the **Boot Config** tab.
3. Select the services you want to enable.
4. Select **Apply**.

Boot Config Field Descriptions

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

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time image.
PrimaryConfigSource	Specifies the primary configuration source.
PrimaryBackupConfigSource	Specifies the backup configuration source to use if the primary does not exist.
EnableFactoryDefaultsMode	Specifies whether the switch uses the factory default settings at startup. • **false**: The node does not use factory default settings at startup. • **fabric**: The node uses the factory default fabric mode settings at startup. Zero Touch Fabric Configuration is enabled. • **noFabric**: The node uses the factory default mode settings at startup. The default value is false. This flag is automatically reset to the default setting after the switch restarts. If you change this parameter, you must restart the switch for the change to take effect.
EnableDebugMode	Enabling the debugmode allows a 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. The default value 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 value is disabled.
EnableRloginServer **Note:** Exception: only supported on VSP 8600 Series.	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.

Table continues…

Name	Description
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 ✱ **Note:** Exception: not supported on VSP 4000 Series or XA1400 Series .	Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. This flag is disabled by default.
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 ✱ **Note:** Exception: only supported on VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	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. In Base Interworking Mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments.
EnableFlowControlMode ✱ **Note:** Exception: not supported on VSP 8600 Series.	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.

Table continues…

Name	Description
	The default is disabled.
AdvancedFeatureBwReservation **Note:** Exception: only supported on VSP 7400 Series and XA1480. Exception: only low level supported on XA1480.	Enables the switch to support advanced features. The default is enabled with low level configuration. The high level means that the switch reserves the maximum bandwidth for the advanced features. The low level means that the switch reserves less bandwidth to support minimum functionality for advanced features. If you change this parameter, you must restart the switch.
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 for VOSS.
EnableSyslogRfc5424Format	Enables or disables the RFC 5424 syslog format. The default is enabled. If the pre-existing configuration file is for a release prior to this enhancement, then the flag is disabled automatically.
NniMstp	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.
EnableIpv6EgressFilterMode	Enables IPv6 egress filters. The default is disabled. If you change this parameter, you must restart the switch.
MasterCPUSlot	Specifies the slot number, either 1 or 2, for the master CPU. The default value is 1.

Table continues…

Name	Description
Note: Exception: only supported on VSP 8600 Series.	
EnableHaCpu **Note:** Exception: only supported on VSP 8600 Series.	Enables or disables the CPU High Availability feature. If you enable or disable HA mode, the secondary CPU automatically resets to load settings from the previously-saved configuration file. The default is enabled.
EnableSavetoStandby **Note:** Exception: only supported on VSP 8600 Series.	Enables or disables automatic save of the configuration file to the standby CPU. The default value is enabled.
Slot	Specifies the slot number.
TftpHash	Enables TFTP hashing.
TftpRetransmit	Set TFTP retransmit timeout counter.
TftpTimeout	Set TFTP timeout counter.
User	Configure host user.
Password	Configure host password.

Reserve Bandwidth for Advanced Features

Use this procedure if you want the switch to support advanced features. When you enable the boot flag, you need to save and reboot with the new configuration.

Before you begin

Product Notice: For VSP 7400 Series, you must ensure your configuration does not include reserved ports before you enable this feature. If the configuration includes reserved ports after you enable this feature and restart the switch, the switch aborts loading the configuration.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Chassis**.
2. Click the **Boot Config** tab.
3. In the **AdvancedFeatureBWReservation** field, select **high** or **low** to enable the boot flag.
4. Click **Apply**.

   A message appears to remind you that the configuration cannot include reserved ports, and that you must save the configuration and reboot the switch for changes to take effect.
5. Click **Yes** to continue or click **No** to cancel the change because the configuration includes reserved ports.

If you clicked No, you can modify your switch configuration to remove the reserved ports and then return to this tab to change the **AdvancedFeatureBWReservation** configuration.

6. Save the configuration, and then reboot the switch.

Enable 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 **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Chassis** tab.
5. In **MTU size**, select either 1950, 9600 or 1522.
6. Click **Apply**.

Configure 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 **Configuration** > **Edit**.
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.

Configure 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 **Configuration** > **Edit** > **Port**.
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.

Configure CP Limit on an Extreme Integrated Application Hosting Port

About this task

Perform this procedure to configure CP Limit functionality to protect the switch from becoming congested by excess data flow through Extreme Integrated Application Hosting (IAH) ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Insight Port**.
2. Select the IAH port you want to configure.
3. Select the **CP Limit** tab.
4. Select **AutoRecoverPort**.
5. Select **Apply**.

CP Limit Field Descriptions

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

Name	Description
AutoRecoverPort	Enables or disables auto recovery of the Extreme Integrated Application Hosting port from action taken by CP Limit or the link flap features. The default is disabled.

Configure 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 **Configuration** > **VRF Context View**.
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 **Configuration** > **Edit**.
7. Click **Mgmt Port**.
8. Click the **IP Address** tab.
9. Click **Insert**.
10. Configure the IP address and mask.
11. Click **Insert**.
12. 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.
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.

Table continues…

Name	Description
	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. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. 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.

Edit 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 **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **General tab**.
5. Modify the appropriate settings.
6. Click **Apply**.

General Field Descriptions

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

Name	Description
Index	Specifies the slot and port number of the management port.
AdminStatus	Configures the administrative status of the device as up (ready to pass packets) or down. The testing state indicates that no operational packets can be passed.
OperStatus	Specifies the operational status of the device.
LicenseControlStatus	Shows the license status of the port: • Locked means the port requires a Port License but one is not present on the switch. • Unlocked means the port requires a Port License and one is present on the switch. • notApplicable means the port does not require a Port License.
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.
IpsecEnable	Enables IPsec on the management port. The default is disabled.
PhysAddress	Shows the MAC address.
AutoNegotiate	Enables or disables Auto-Negotiation for this port. The default varies depending on the platform: • VSP 4000 Series - Enabled • VSP 4900 Series - Enabled • VSP 7200 Series - Disabled • VSP 7400 Series - Enabled • VSP 8200 Series - Enabled • VSP 8400 Series - Enabled • VSP 8600 Series - Enabled (except 10 Gbps SFP+ ports)
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.

Configure 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 **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **IPv6 Interface** tab.
5. Click **Insert**.
6. Edit the fields as required.
7. Click **Insert**.
8. Click **Apply**.

IPv6 Interface field descriptions

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

Name	Description
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

Table continues…

Name	Description
	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.

Configure 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 **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **IPv6 Addresses** tab.
5. Click **Insert**.
6. In the **Addr** box, type the required IPv6 address for the management port.
7. In the **AddrLen** box, type the number of bits from the IPv6 address you want to advertise.
8. Click **Insert**.
9. Click **Apply**.

IPv6 Addresses field descriptions

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

Name	Description
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.

Table continues…

Name	Description
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 **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **CP Limit** tab.
5. Select **AutoRecoverPort** to activate auto recovery of the port from the action taken by SLPP shutdown features. The default value is disabled.
6. Click **Apply**.

Edit 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 **Configuration** > **Edit**.
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	Identifies the port as a serial port.
BaudRate	Specifies the baud rate of this port. Different hardware platforms support different baud rates, which also impacts the default value for each hardware platform: • VSP 4000 Series — 9600 • VSP 4900 Series — 115200 • VSP 7200 Series — 9600 • VSP 7400 Series — 115200 • VSP 8000 Series — 9600 • VSP 8600 Series — 115200 • XA1400 Series — 115200
DataBits	Specifies the number of data bits, for each byte of data, this port sends and receives. The default is eight.

Enable 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 **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. To enable port lock, select the **Enable** check box.
5. Click **Apply**.

Port Lock field descriptions

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

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

Lock 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 **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. In the **LockedPorts** box, click the ellipsis **(...)** button.
5. Click the desired port or ports.
6. Click **Ok**.
7. In the Port Lock tab, click **Apply**.

Port Lock field descriptions

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

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

Configure Power on Module Slots

About this task

Use this procedure to control whether or not to supply power to specific slots that contain either switch fabric modules or input/output modules. By default, power is available to all slots.

After enabling power to specific input/output module slots, you can also configure the priority in which they are powered on. For more information, see Configure Slot Priority on page 214.

Note:

This feature is not available for hardware platforms with fixed configurations. It is only available for platforms where the user can install modules in slots.

Procedure

1. In the Device Physical View tab, select a module.
2. In the navigation pane, expand **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Card** tab.
5. In the **SlotPower** field, select the priority level: *on* or *off*.
6. Click **Apply**.

Configure Slot Priority

Note:

This procedure only applies to VSP 8600 Series.

About this task

Configure slot priority to specify which slots you want to shut down if there is insufficient power available in the chassis. By default, power is available to all slots, and the slots have the following priority:

- Slots 1, 2, SF1, SF2, and SF3 must always be *Critical* so you cannot configure them.
- Slots 3-8 are *High* by default, but you can configure any of them to *Low*.

Note:

Power is always supplied to critical slots first which are the CP modules, SF modules, and fan trays.

The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first) and interface slots shut down before CP, SF modules, and fan tray slots.

For example, if slot 3 has a `low` priority and slots 4 and 5 have a `high` priority, the slot shutdown priority is as follows: 4, 5, 3. Slot 3 has the lowest priority because it was configured as `low` so it would be shut down first. Slots 4 and 5 have the same priority, but slot 5 shuts down before slot 4 because slot 4 has a higher slot number.

Procedure

1. In the Device Physical View tab, select a module.
2. In the navigation pane, expand **Configuration** > **Edit**.

3. Click **Card**.
4. Click the **Card** tab.
5. In the **PowerManagementPriority** field, select the priority level: *high* or *low*.
6. Click **Apply**.

Viewe 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 **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Power Info** tab.

Power Info field descriptions

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

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

View Power Status

About this task

Perform the following procedure to view the power consumption of the modules in the chassis.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Power Consumption** tab.

Power consumption field descriptions

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

Name	Description
Index	Displays an index value that identifies the component.
PowerStatus	Displays the power status: on or off.
BasePower	Displays the base power required for the slot.
ConsumedPower	Displays the actual consumed power for the slot. This value is 0 if the power status is off.
PowerPriority	Displays the priority of the slot for power management.
SlotDescription	Displays the slot number.
CardDescription	Identifies the type of module in the slot.

View Fan Tray Information

View fan tray information to see manufacturing information about the fans.

✱ **Note:**

Not all fields are supported on all hardware platforms.

Procedure

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

Fan Tray Info field descriptions

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

Name	Description
TrayId	Specifies the fan tray ID.
Description	Shows a description of the fan tray.
SerialNumber	Shows the serial number for the fan tray.
PartNumber	Shows the part number for the fan tray.
FlowType	Specifies whether the air flow is front-to-back or back-to-front.

View USB Port Information

About this task

Perform this procedure to view information about the USB port on the switch.

Note:

This information may not apply to your hardware model. For more information about your model features, see your hardware documentation.

Procedure

1. In the Device Physical View, select the USB port.
2. In the navigation pane, expand **Configuration** > **Edit**.
3. Click **USB Port**.
4. Click the **General** tab.

General field descriptions

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

Name	Description
UsbStatus	Displays the current status of USB storage: either present or notPresent.
UsbDescription	Displays a description of the USB storage.

View USB Device Information

About this task

Perform this procedure to view information about an inserted USB device.

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, expand **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **USB** tab.

USB field descriptions

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

Name	Description
SlotDescription	Specifies the slot type information.
VendorId	Specifies the vendor ID for the inserted USB device.
Manufacturer	Specifies the manufacturer of the inserted USB device.
ProductId	Specifies the product ID of the inserted USB device.
ProductName	Specifies the product name of the inserted USB device.
SerialNumber	Specifies the serial number of the inserted USB device.
Revision	Specifies the release number of the inserted USB device.
MaxCurrent	Specifies the maximum power as defined by the specification for the inserted USB device. The units of measurement are milliamps.

View 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 **Configuration** > **Edit** > **Diagnostics**.
2. Click **Topology**.
3. Click the **Topology** tab.

Topology field descriptions

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

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

View 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 **Configuration** > **Edit** > **Diagnostics**.
2. Click **Topology**.
3. Click the **Topology Table** tab.

Topology Table Field Descriptions

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

Name	Description
Slot	Specifies the slot number in the chassis that received the topology message.
Port	Specifies the port that received the topology message.
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.

Configure 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 **Configuration** > **Edit** > **Chassis**.
2. Click the **Force Msg Patterns** tab.
3. Click **Insert**.
4. In the **PatternId** field, enter a pattern ID number.
5. In the **Pattern** field, enter a message control pattern.
6. Click **Insert**.

Force Msg Patterns Field Descriptions

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

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

View Fan Information

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

Note:

This tab does not appear on the VSP 8600 Series switch.

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 **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Fan Info** tab.

Fan Info field descriptions

Use the data in the following tables to use the Fan Info tab.

Name	Description
Description	Specifies a description of the fan location.
OperStatus	Specifies the operation status of the fan.
OperSpeed	Specifies the actual fan speed.

Configure Ports Speeds for All VIM Ports

Note:

This procedure only applies to VSP 4900 Series.

Configure all of the ports on an installed Versatile Interface Module (VIM) to operate at the same speed.

Note:

Some VIMs must operate with all ports at the same speed, while others can operate with ports at different speeds. For more information, see Release Notes for VOSS. You can configure VIM ports speed only on VIMs that must operate with all ports at the same speed.

Before you begin

Install the VIM before performing this procedure.

About this task

Use this procedure to configure the speed of all ports in a multi-port VIM to operate at either 10 Gbps or 25 Gbps.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Chassis**.
3. Select the **VIM** tab.
4. Select **mbps10000** or **mbps25000**.
5. Select **Apply**.

VIM Field Descriptions

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

Name	Description
AdminSpeed	• **mbps10000**: Configures all ports in a multi-port VIM to operate at 10 Gbps.

Name	Description
	• **mbps25000**: Configures all ports in a multi-port VIM to operate at 25 Gbps. The default is 25 Gbps.

View Modular SSD Information

About this task

Perform this procedure to display information about an installed Solid State Drive (SSD) on a switch.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Chassis**.
3. Select the **SSD** tab.

SSD Field Descriptions

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

Name	Description
ProductName	Specifies Solid State Drive (SSD) product name.
VendorName	Specifies the SSD vendor.
ManufactureDate	Specifies the date on which the SSD was manufactured.
SerialNum	Specifies the SSD serial number.
PartNum	Specifies the SSD part number.
DeviceVersion	Specifies the version of the SSD.
TotalSize	Specifies the total memory size of the SSD.

Prepare a slot for IOC Module Preconfiguration using EDM

About this task

Use this procedure to designate a slot in the switch for IOC Module Preconfiguration. A slot can be designated for only one module type at a time.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Card Preconfig**.
2. Click **Insert**.
3. Enter the slot number in the **Slot** field.

4. Select the IOC Module type in the **CardType** field.
5. Select the **Lock** field to lock the slot to the specified IOC Module type.
6. Click **Insert**.

Card Preconfig Field Descriptions

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

Field	Description
Slot	Specifies the slot number designated for pre-configuration.
CardType	Specifies the type of the IOC Module designated for the slot.
Lock	If selected, the slot is locked to only accept the type of IOC Module designated.

Chapter 9: Power over Ethernet Fundamentals

Table 30: Power over Ethernet product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Power over Ethernet (PoE)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1 VSP4900-48P and first 12 ports of VSP4900-12MXU-12XE only
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	Not Applicable
	XA1400 Series	Not Supported
PoE/PoE+ allocation using LLDP	VSP 4450 Series	VOSS 5.1
	VSP 4900 Series	VOSS 8.1 VSP4900-48P and first 12 ports of VSP4900-12MXU-12XE only
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	Not Applicable
	XA1400 Series	Not Supported
Fast PoE	VSP 4450 Series	Not Applicable
	VSP 4900 Series	VOSS 8.1 VSP4900-48P and first 12 ports of VSP4900-12MXU-12XE only
	VSP 7200 Series	Not Applicable

Table continues…

Feature	Product	Release introduced
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	Not Applicable
	XA1400 Series	Not Supported
Perpetual PoE	VSP 4450 Series	Not Applicable
	VSP 4900 Series	VOSS 8.1 VSP4900-48P and first 12 ports of VSP4900-12MXU-12XE only.
	VSP 7200 Series	Not Applicable
	VSP 7400 Series	Not Applicable
	VSP 8200 Series	Not Applicable
	VSP 8400 Series	Not Applicable
	VSP 8600 Series	Not Applicable
	XA1400 Series	Not Supported

Power over Ethernet (PoE) is the implementation of IEEE 802.3af and 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 VSP 4900 Series Switches: Hardware Installation Guide.

The switch uses the Dynamic Power Allocation scheme when supplying power to devices. Only the power being consumed by the device is allocated, improving efficiency and enabling support for more number of devices.

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.

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.

Important:

- After you enable Fast PoE or Perpetual PoE or both, you must save the running configuration file.
- If Fast PoE or Perpetual PoE are enabled and you change any other global or port-specific PoE settings (for example, power limits, or port power priority), you must resave the running configuration file.

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 limits the amount of power supplied on a particular port and varies across different hardware platforms. If a PD requires more than the configured limit, the device will not connect properly or is forced to run at a lower limit.

The following table lists the power limit for different hardware platforms:

Table 31: Power Limits

Platform	Power Limit
VSP 4000 Series	32 watts
VSP 4900-48P	32 watts
VSP 4900-12MXU-12XE	64 watts

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 32: 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 33: 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

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 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.

Fast PoE and Perpetual PoE

Fast PoE minimizes the PoE controller recovery time in case of a power failure. With Fast PoE, the PoE controller initializes the moment the switch powers on, which results in a faster recovery period.

Perpetual PoE provides uninterrupted power to all connected devices during a switch reboot.

Important:

- After you enable Fast PoE or Perpetual PoE or both, you must save the running configuration file.
- If Fast PoE or Perpetual PoE are enabled and you change any other global or port-specific PoE settings, you must resave the running configuration file.

Power over Ethernet Configuration using CLI

This section provides details to configure PoE settings using CLI.

Important:

- After you enable Fast PoE or Perpetual PoE or both, you must save the running configuration file.
- If Fast PoE or Perpetual PoE are enabled and you change any other global or port-specific PoE settings, you must resave the running configuration file.

Disabling PoE on a port

About this task

Perform the following procedure to disable PoE on a port. The Ethernet connected device does not receive any power over Ethernet if you shutdown PoE on the 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 the 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

Perform the following procedure to configure the PoE powered device (PD) detection type. You can enable 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. Normal power and high power devices are supported in 802.3at.

❗ **Important:**

Power delivery is interrupted and all PoE PDs are reset if you change from 802.3at to 802.3af. Power delivery is not interrupted if you change 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

The following table defines parameters for the **`poe-pd-detect-type`** command.

Variable	Value
{802dot3af | 802dot3af_and_legacy | 802dot3at | 802dot3at_and_legacy | 802dot3bt_type3 | 802dot3bt_type4}	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 • 802dot3bt_type3: Set PD detection mode in 802dot3bt Type3 • 802dot3bt_type4: Set PD detection mode in 802dot3bt Type4

Configuring PoE Power Usage Threshold

About this task

Perform the following procedure to configure the PoE power usage threshold limit globally as a percentage on the switch. The switch logs a warning message when a PoE PD power usage exceeds the configured threshold. The switch logs an informational message when a PoE PD power usage is below the configured threshold.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the power usage threshold:

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

Variable Definitions

The following table defines parameters for the **poe-power-usage-threshold** command.

Variable	Value
<1–99>	Specifies the PoE usage threshold in the range of 1—99 percent.

Configure Power Limits for Channels

About this task

Perform the following procedure to configure the PoE power limit for specific ports or channels. You can limit the PoE wattage available from an individual port or list of ports.

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 the 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>] <power_limit>
   ```

Variable definitions

The following table defines parameters for the **poe-limit** command.

Variable	Value
<portlist>	Identifies the ports on which the limit is set.
<power_limit>	Specifies the configurable power limit, in watts on a particular port. To see the available range for the switch, use the CLI Help.

Configuring Port Power Priority

About this task

Perform the following procedure to configure the PoE power priority for a port or list of ports. You can configure the PoE power priority of ports to manage availability of the connected PDs. If the switch needs to shut down PDs because PoE exceeds the power limit threshold, low priority devices are shut down before high priority, and high priority are shut down before critical.

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 the 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

The following table defines parameters for the **`poe-priority`** command.

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

Enable Fast PoE Globally

About this task

Perform this procedure to enable Fast PoE on the switch. After you enable Fast PoE, you must save the running configuration file.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable Fast PoE:

   ```
   poe fast-poe-enable
   ```

3. Save the configuration file:

   ```
   save config
   ```

Enable Perpetual PoE Globally

About this task

Perform this procedure to enable Perpetual PoE on the switch. After you enable Perpetual PoE, you must save the running configuration file.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable Perpetual PoE:

   ```
   poe perpetual-poe-enable
   ```

3. Save the configuration file:

   ```
   save config
   ```

Enable Fast PoE on a Port

About this task

Perform this procedure to enable Fast PoE on a specific copper port of the switch. After you enable Fast PoE, you must save the running configuration file.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

2. Enable Fast PoE on the copper port:

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

3. Save the configuration file:

   ```
   save config
   ```

Variable Definitions

The following table defines parameters for the **fast-poe-enable** command.

Variable	Value
port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Specifies the port or ports to be configured.

Enable Perpetual PoE on a Port

About this task

Perform this procedure to enable Perpetual PoE on a specific copper port of the switch. After you enable Perpetual PoE, you must save the running configuration file.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

2. Enable Fast PoE on the copper port:

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

3. Save the configuration file:

   ```
   save config
   ```

Variable Definitions

The following table defines parameters for the **fast-poe-enable** command.

Variable	Value
port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Specifies the port or ports to be configured.

Display Global PoE Configuration

About this task

Perform the following procedure to display the global PoE configuration. You can view the global PoE status, power consumption, power limit threshold, and more.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the global 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
Fast POE Status            : Enabled
Perpetual POE Status       : Enabled
POE Firmware Version:      : 3.0.0.6
```

Displaying PoE Port Status

About this task

Perform the following procedure to display the PoE status for each port. You can use this information to view the status, classification, watts, and priority for each PoE port.

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

Perform the following procedure to display the PoE power measurement. You can view the voltage, amperage, and wattage for every PoE port. PoE ports without a PD in use are measured as zeros.

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.

Configure PoE Globally

About this task

Configure PoE usage threshold and device type settings, and enable Fast PoE and Perpetual PoE globally on a switch.

Important:

- After you enable Fast PoE or Perpetual PoE or both, you must save the running configuration file.
- If Fast PoE or Perpetual PoE are enabled and you change any other global or port-specific PoE settings, you must resave the running configuration file.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Chassis**.
3. Select the **PoE** tab.
4. Configure the fields as required.
5. Select **Apply**.

PoE Field Descriptions

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

Name	Description
Power(watts)	Specifies the nominal power of the Power Sourcing Entity expressed in Watts.
OperStatus	Specifies the operational status of the main Power Sourcing Entity.
ConsumptionPower(watts)	Specifies the measured usage power expressed in Watts.

Table continues…

Name	Description
UsageThreshold%	Configures the usage threshold in percent for comparing the measured power and initiating an alarm if the threshold is exceeded.
PoweredDeviceDetectType	Configures the mechanism used to detect powered ethernet devices attached to a powered ethernet port. The options are: • 802.3af • 802.3afAndLegacySupport • 802.3at • 802.3atAndLegacySupport
PowerPresent	Specifies the current power source present on the switch. Available power sources are AC and DC. A value of **acOnly** indicates that the only power supply is AC. A value of **dcOnly** indicates that the only power supply is DC. A value of **acDc** indicates that the two power supplies, AC and DC are supplying power.
FastPoeEnable **Note:** Exception: only supported on VSP 4900 Series.	Enables Fast PoE on the switch. The default is disabled.
PerpetualPoeEnable **Note:** Exception: only supported on VSP 4900 Series.	Enables Perpetual PoE on the switch. The default is disabled.

Configure PoE on Ports

About this task

Enable or disable PoE on a port, and configure PoE priority and power limit settings.

Important:

If Fast PoE or Perpetual PoE are enabled and you change any other global or port-specific PoE settings, you must resave the running configuration file.

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 **Configuration** > **Edit** > **Port**.

3. Select **General**.
4. Select the **PoE** tab.
5. Configure the fields as required.
6. Click **Apply**.

PoE Field Descriptions

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

Name	Description
AdminEnable	Enabled or disables PoE on this port.
FastPoeEnable **Note:** Exception: only supported on VSP 4900 Series.	Enables or disables Fast PoE on this port. The default is disabled.
PerpetualPoeEnable **Note:** Exception: only supported on VSP 4900 Series.	Enables or disables Perpetual PoE on this port. The default is disabled.
DetectionStatus	Specifies the operational status of the power device detecting mode on this 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 (OtherFault)—a power-specific fault has been detected on the port • Test—detecting device is in test mode
PowerClassifications	Specifies the power classification of the device connected to this port. Power classification tags 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	Configures the power priority for this port: • critical • high • low

Table continues…

Name	Description
PowerLimit(Watts)	Configures the maximum power that the switch can supply to a port.
Voltage(volts)	Specifies the power measured in volts.
Current(amps)	Specifies the power measured in amps.
Power(Watts)	Specifies 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).

Configure 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 **Configuration** > **Device**.
2. Click **Preference Setting**.
3. Enable polling or hot swap detection.
4. Configure the frequency to poll the device.
5. Click **Apply**.

Preference Setting field descriptions

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

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

View Module Information

View the administrative status for modules in the chassis.

About this task

This command is not available for hardware platforms with fixed configurations. It is only available for platforms where the user can install modules in slots.

Procedure

1. In the Device Physical View tab, select a module slot.
2. In the navigation pane, expand **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Card** tab.

Card field descriptions

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

Name	Description
CardType	Displays the model number of the module.
CardDescription	Shows a description of the installed module.
SerialNum	Shows the serial number for the installed module.
PartNumber	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.
PowerManagementPriority	Specifies the slot priority for power management as either `high` or `low`.

View Module Storage Usage

View the storage usage for modules in the chassis.

About this task

You cannot perform this procedure on hardware platforms with fixed configurations. It is only available for platforms where you can install modules in slots.

Procedure

1. In the Device Physical View tab, select a module slot.
2. In the navigation pane, expand **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Storage Usage** tab.

Storage Usage Field Descriptions

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

Name	Description
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.

View Power Supply Parameters

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

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Power Supply**.

Details Field Descriptions

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

Name	Description
Id	Specifies the ID number. This field is not supported on all hardware platforms.
Type	Describes the type of power used.
Description	Provides a description of the power supply.

Table continues…

Name	Description
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	Displays 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
OutputWatts	Displays the output power of this power supply.
InputOperLineVoltage	Displays the operating input line voltage. If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage shows the low 110v value. This field is not supported on all hardware platforms.
InputPower	Displays the input power of this power supply. This field is not supported on all hardware platforms.

View Power Supply Information

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

About this task

This tab does not appear in all hardware platforms.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Power Supply Information**.

Details Field Descriptions

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

Name	Description
Id	Specifies the ID number. This field is not supported on all hardware platforms.
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	Displays 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
OutputWatts	Displays the output power of this power supply.
InputOperLineVoltage	Displays the operating input line voltage. If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage shows the low 110v value. This field is not supported on all hardware platforms.
InputPower	Displays the input power of this power supply. This field is not supported on all hardware platforms.

View System Temperature Information

View information about the temperature for each sensor on the device.

The system triggers an alarm when one of the zones exceeds the threshold temperature value.

Note:

This procedure does not apply to all hardware models.

Procedure

1. In the Device Physical View tab, select the chassis.
2. In the navigation pane, expand **Configuration** > **Edit**.

3. Click **Chassis**.
4. Click the **System Temperature** tab.

System Temperature field descriptions

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

Name	Description
SensorIndex	Specifies the range of sensors on the device.
SensorDescription	Specifies the name of the sensor.
Temperature (degrees celsius)	Specifies the sensor temperature measured in Celsius degrees.
WarningThreshold	Specifies the temperature value of the warning threshold for the sensor. When the temperature crosses the warning threshold a warning message is generated.
CriticalThreshold	Species the temperature value of the critical threshold for the sensor. When the temperature crosses the critical threshold, a critical message is generated or the system shuts down, depending on hardware capability.
Status	Specifies the current temperature status based on the warning and critical thresholds.

View Temperature on the Chassis

You can view information about the temperature on the chassis.

Note:

This tab appears only on the VSP 8600 Series switch.

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 **Configuration** > **Edit**.

3. Click **Chassis**.
4. Click the **Temperature** tab.

Temperature field descriptions

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

Name	Description
CpuTemperature	Current CPU temperature in Celsius.
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

Table 34: Domain Name Service product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Domain Name Service (DNS) client (IPv4)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
DNS client (IPv6)	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	Not Supported

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.

The DNS client tracks any server addresses or domain names provided from a DHCP server. If a DHCP server provides info to the DNS client, the DNS configuration is classified as dynamic. You can manually delete dynamic DNS entries, but cannot manually add dynamic DNS entries. You can view the Dynamic DNS entries with **`show ip dns`** or **`show sys dns`**. Dynamic DNS entries are not saved in the configuration file. The status monitoring of DNS occurs every 60 seconds.

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 primary, secondary, or tertiary DNS servers:

   ```
   ip name-server <primary|secondary|tertiary> WORD<0-46>
   ```

4. **(Optional)** Delete addresses for primary, secondary, or tertiary DNS servers:

   ```
   no ip name-server <primary|primary-dynamic|secondary|secondary-
   dynamic|tertiary|tertiary-dynamic> WORD<0-46>
   ```

5. View the DNS client system status:

   ```
   show ip dns
   ```

Example

```
Switch:1> enable
```

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

Add addresses for a tertiary DNS server:

```
Switch:1(config)# ip name-server tertiary 254.104.201.141
```

Delete address for a secondary dynamic DNS server:

```
Switch:1(config)#no ip name-server secondary-dynamic 192.0.2.12
```

Variable Definitions

The following table defines parameters for the **`ip domain-name`** command.

Variable	Value
WORD<0–255>	Configures the default domain name.

Variable	Value
	WORD<0–255> is a string 0–255 characters.

The following table defines parameters for 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 192.0.2.1
```

Variable Definitions

The following table defines parameters for 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**.

Configure 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 **Configuration** > **Edit** > **Diagnostics**.
2. Click **DNS**.
3. Click the **DNS Servers** tab.
4. Click **Insert**.
5. In the **DnsServerListType** box, select the DNS server type.
6. In the **DnsServerListAddressType** box, select the IP version.
7. In the **DnsServerListAddress** box, enter the DNS server IP address.
8. Click **Insert**.

DNS Servers Field Descriptions

Use the data in the following table to use the **DNS Servers** tab.

Name	Description
DnsServerListType	Configures the DNS server as primary, secondary, or tertiary. OR Removes a DNS server as primary, primaryDynamic, secondary, secondaryDynamic, tertiary, or tertiaryDynamic.
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.

Query 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 **Configuration** > **Edit** > **Diagnostics**.
2. Click **DNS**.
3. Click the **DNS Host** tab.
4. In the **HostData** text box, enter the DNS host name, IPv4 or the IPv6 address.
5. Click **Query**.

DNS Host Field Descriptions

Use the data in the following table to use the **DNS Host** tab.

Name	Description
HostData	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: Power Savings

Power savings allow you to reduce network infrastructure power consumption during periods of low data activity without impacting network connectivity.

Depending on the power saving option you choose, you can implement power savings on a switch-wide, or on a per-port basis. The following power saving options are supported:

- Energy Saver (switch-wide or per-port)
- Energy Efficient Ethernet (EEE) (per-port only)

You must choose either Energy Saver, or Energy Efficient Ethernet (EEE)—you cannot use both options together.

The following sections describe the Energy Saver and Energy Efficient Ethernet (EEE) features, and how to configure them.

Power Savings Fundamentals

Energy Saver

Table 35: Energy Saver product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Energy Saver	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1 VSP4900-48P and ports 1/1 to 1/12 onVSP4900-12MXU-12XE only
	VSP 7200 Series	VOSS 7.0 VSP 7254XTQ only
	VSP 7400 Series	Not Supported

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	Not Supported
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

To redure direct power consumption by up to 40%, Energy Saver uses intelligent-switching capacity reduction in off-peak mode by controlling port link speeds and optionally powering off low priority PoE devices during off-peak periods. You can schedule Energy Saver to activate during multiple specific time periods. These time periods can be as short as one minute, or can last a week, a weekend, or individual days.

Note:

- Energy Saver is supported only on copper ports that have auto-negotiation enabled on them.
- If auto-negotiation is disabled on a port and a custom port speed is configured, Energy Saver will not change the speed of that port.

Important:

- Configuring the port link speed to a low value impacts the overall network performance. The best practice is to use the Energy Saver feature during the hours when the network is not overburdened.
- If a switch is reset while Energy Saver is activated, the PoE power-saving calculation might not accurately reflect the power saving, and in some cases might display zero savings. This problem occurs because the switch did not have sufficient time to record PoE usage between the reset of the switch and the reactivation of Energy Saver. When Energy Saver is next activated, the PoE power saving calculation is correctly updated.
- When Energy Saver is active and you replace a unit, that unit will not be in Energy Saver mode. You must configure Energy Saver directly after replacing a unit.

Interaction with PoE

Energy Saver can use Power over Ethernet (PoE) port-power priority levels to shut down low-priority PoE ports and provide power savings. The power consumption savings of each switch is determined by the number of ports with Energy Saver enabled, and by the power consumption of PoE ports that are powered off. If Energy Saver is disabled on a port, the port is not powered off, irrespective of the PoE configuration. Energy Saver turns off the power to a port only when PoE is enabled globally, the port Energy Saver is enabled, and the PoE priority for the port is configured to Low.

Configuration Fundamentals

To fully configure and use Energy Saver, you must first enable Energy Saver on ports, create a schedule, and then enable Energy Saver globally.

Alternatively, you can configure Energy Saver using the Efficiency Mode quick configuration method, which enables Energy Saver on all ports, creates a default schedule, and enables Energy Saver globally.

You can manually deactivate and reactivate Energy Saver at any time, without affecting the port configurations.

Note:

- Energy Saver is supported only on copper ports that have auto-negotiation enabled.
- Network Time Protocol (NTP) must be enabled and configured to use Energy Saver.

Energy Efficient Ethernet

Table 36: Energy Efficient Ethernet product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Energy Efficient Ethernet (EEE)	VSP 4450 Series	Not Supported
	VSP 4900 Series	VOSS 8.1 All fixed ports on VSP4900-48P and ports 1/1-1/12 on VSP4900-12MXU-12XE
	VSP 7200 Series	Not Supported
	VSP 7400 Series	Not Supported
	VSP 8200 Series	Not Supported
	VSP 8400 Series	VOSS 8.1 8424GT
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

Energy Efficient Ethernet (EEE) supports the IEEE 802.3az standard for power savings in Ethernet networks for a select group of physical layer devices. A physical device that can support low power idle (LPI) mode is considered EEE-capable. Legacy devices that do not support EEE can be made EEE-compliant with an EEE-compliant PHY and an SDK version that allows the MAC device to interact with the PHY EEE functionality.

In a typical configuration, the EEE protocol communicates with the switch and the physical device to determine when to enter LPI mode during a period of inactivity, and to exit LPI mode when data transmission resumes.

Note:

EEE is supported only on copper ports that have auto-negotiation enabled on them.

Power Savings Configuration Using CLI

Configure Energy Saver or Energy Efficient Ethernet using the command line interface (CLI).

Enable Energy Saver on Ports

About this task

Perform this procedure to enable Energy Saver on a specific port or range of ports.

Before you begin

- If you have previously enabled Energy Saver globally, you must disable it globally before enabling Energy Saver on individual ports.
- If you have previously enabled Efficiency Mode, you must disable it before enabling Energy Saver on individual ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   Note:

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

2. Enable Energy Saver 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 slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

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

Example

Enable energy savings on slot 1 port 2:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 1/2
Switch:1(config-if)#energy-saver port 1/2 enable
```

Next steps

Configure an Energy Saver schedule.

Variable Definitions

The following table defines parameters for the **`energy-saver`** command.

Variable	Value
enable	Enables energy savings on ports. The default is disabled.
{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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Create an Energy Saver Schedule

About this task

Perform this procedure to configure scheduled time intervals during which the switch will operate in low power state. This time interval can be for a week, weekend, or individual days.

Note:

You can configure a maximum of 84 entries in the Energy Saver schedule.

Before you begin

- If you have previously enabled Energy Saver globally, you must disable it globally before creating a schedule.
- If you have previously enabled Efficiency Mode, you must disable it before creating a schedule. You cannot change the default Efficiency Mode schedule entries when Efficiency Mode is enabled.
- You must enable Energy Saver on every port affected by the schedule.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the Energy Saver schedule:

   ```
   energy-saver schedule {friday | monday | saturday | sunday |
   thursday | tuesday | wednesday | weekday | weekend} <hhmm> {activate
   | deactivate}
   ```

Example

Configure an Energy Saver schedule:

```
Switch:1>enable
Switch:1# configure terminal
Switch:1(config)#energy-saver schedule weekend 0735 activate
Switch:1(config)#energy-saver schedule monday 0600 deactivate
```

Next steps

Enable Energy Saver globally.

Variable Definitions

The following table defines parameters for the **`energy-saver schedule`** command.

Variable	Value
{activate | deactivate}	Activates or deactivates the scheduled event.
<hhmm>	Specifies the hour and minutes to enable Energy Saver feature on the switch.
{friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekday | weekend}	Specifies the day(s) to enable Energy Saver feature on the switch.

Enable Energy Saver Globally

About this task

Perform this procedure to enable Energy Saver globally on the switch. You can optionally configure PoE power savings, to power off low priority PoE devices during off-peak times.

Before you begin

- You must enable Energy Saver on individual ports.
- You must create an Energy Saver schedule.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. **(Optional)** Configure PoE power savings:

   ```
   energy-saver poe-power-saving
   ```

   Note:

   You must configure PoE power savings before you enable Energy Saver globally.

3. Enable Energy Saver:

   ```
   energy-saver enable
   ```

Example

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

```
Switch:1(config)#energy-saver poe-power-saving
```

```
Switch:1(config)#energy-saver enable
```

Variable Definitions

The following table defines parameters for the **`energy-saver`** command.

Variable	Value
enable	Enables Energy Saver feature. The default is disabled.
poe-power-saving	Enables PoE power saving. The default is disabled.

Enable and Configure Energy Saver using Quick Configuration

About this task

Perform this procedure to enable and configure Energy Saver globally using the quick configuration Efficiency Mode. Efficiency Mode automatically configures the following:

- enables Energy Saver on all ports.
- creates a default schedule with a weekday schedule of Energy Saver activated from 6:00 p.m. to 7:30 a.m., and during weekends. You cannot change this default schedule while Efficiency Mode is enabled.
- enables Energy Saver globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable efficiency mode:

   ```
   energy-saver efficiency-mode
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#energy-saver efficiency-mode
```

Variable Definitions

The following table defines parameters for the **`energy-saver`** command.

Variable	Value
efficiency-mode	Enables efficiency mode. The default is disabled.

Activate or Deactivate Energy Saver Manually

About this task

Perform this procedure to activate or deactivate Energy Saver on the switch at any time. Energy Saver is deactivated by default.

Activating Energy Saver reduces the port speed to the minimum value supported by the switch and enables PoE power saving, even if PoE is globally disabled. Deactivating Energy Saver restores the previous configuration.

Before you begin

Before you can change any previously saved Energy Saver settings, you must disable Energy Saver globally.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Activate or deactivate Energy Saver:

   ```
   energy-saver {activate | deactivate}
   ```

Example

```
Switch:1 enable
```

Activate Energy Saver:

```
Switch:1# energy-saver activate
```

Deactivate Energy Saver:

```
Switch:1# energy-saver deactivate
```

Variable Definitions

The following table defines parameters for the **`energy-saver`** command.

Variable	Value
activate	Activates Energy Saver manually.
deactivate	Deactivates Energy Saver manually.

Energy Saver Show Commands

Use the procedures in this section to display specific information about Energy Saver configuration on the switch.

Display Energy Saver Global Information

About this task

Perform this procedure to display information about Energy Saver global configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display global configuration:

   `show energy-saver global`

Example

```
Switch:1#show energy-saver global
Energy Saver:                       Disabled
Energy Saver PoE Power Saving Mode: Disabled
Energy Saver Efficiency-Mode Mode:  Disabled
Day/Time:                           Wednesday 02:31:12
Current Energy Saver state:         Energy Saver is Inactive
```

Display Energy Saver Interface Information

About this task

Perform this procedure to display information about Energy Saver configuration on the ports.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display information about all ports or specify a particular port:

   `show energy-saver interface` [*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]

Example

```
Switch:1>enable
Switch:1#show energy-saver interface
Port ES State PoE Savings PoE Priority
----- --------- ----------- ------------
1/1       Enabled   Enabled     Low
1/2       Enabled   Enabled     Low
1/3       Enabled   Enabled     Low
1/4       Enabled   Enabled     Low
1/5       Enabled   Enabled     Low
1/6       Enabled   Enabled     Low
1/7       Enabled   Enabled     Low
1/8       Enabled   Enabled     Low
1/9       Enabled   Enabled     Low
1/10      Enabled   Enabled     Low
1/11      Enabled   Enabled     Low
1/12      Enabled   Enabled     Low
1/13      Disabled  N/A         N/A
1/14      Disabled  N/A         N/A
1/15      Disabled  N/A         N/A
```

Display Energy Saver Power Savings Information

About this task

Perform this procedure to display information about Energy Saver power savings on the switch.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display information about energy savings:

   ```
   show energy-saver savings
   ```

Example

```
Switch:1#show energy-saver savings
----------------------------------------------------------
Unit Model        Switch Capacity        Saving PoE Saving
----------------------------------------------------------
8404C                0.0 watts                   N/A
==========================================================
```

Display Energy Saver Schedule Information

About this task

Perform this procedure to display information about Energy Saver schedules configured on the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display information about Energy Saver schedules:

   ```
   show energy-saver schedule
   ```

Example

```
Switch:1#show energy-saver schedule
----------------------------
Day       Time  Action
----------------------------
Monday    18:00 Activate
Monday    07:00 Deactivate
```

Enable Energy Efficient Ethernet (EEE)

About this task

Perform this procedure to enable Energy Efficient Ethernet (EEE) on a port. The default is disabled.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

Note:

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

2. Enable Energy Efficient Ethernet:

```
energy-saver eee enable
```

Power Savings Configuration Using EDM

Use the following procedures to configure either Energy Saver or Energy Efficient Ethernet EEE using Enterprise Device Manager (EDM).

Enable Energy Saver Globally

About this task

Perform this procedure to enable Energy Saver globally.

Procedure

1. In the navigation pane, expand **Configuration** > **Power Management**.
2. Click **Energy Saver**.
3. Click the **Energy Saver Globals** tab.
4. Configure the fields as required.
5. Click **Apply**.

Energy Saver Globals Field Descriptions

Name	Description
EnergySaverEnabled	Enables Energy Saver globally on the switch. The default is disabled.
PoePowerSavingEnabled	Enables Energy Saver PoE power saving. The default is disabled.
EfficiencyModeEnabled	Enables Energy Saver efficiency mode. The default is disabled. Efficiency mode enables Energy Saver globally and on all ports, it also enables PoE power saving. It also creates a weekday schedule that starts at 6:00 p.m. and ends at 7:30 a.m., and during the weekend Energy Saver is always activated.

Table continues…

Name	Description
EnergySaverActive	Activates Energy Saver on the switch. Energy Saver is deactivated by default.

Configure Energy Saver Schedule

About this task

Perform this procedure to configure a scheduled time interval during which the switch will operate in low power state. This time interval can be for a week, weekend, or individual days.

✱ **Note:**

- You can configure maximum 84 entries in the Energy Saver schedule.
- If efficiency mode is enabled, you cannot configure any other entries in theEnergy Saver schedule.

Before you begin

- You must disable Energy Saver globally.
- You must enable Energy Saver on every port affected by the schedule.
- You must deactivate Energy Saver efficiency-mode.

Procedure

1. In the navigation pane, expand **Configuration** > **Power Management**.
2. Click **Energy Saver**.
3. Click the **Energy Saver Schedules** tab.
4. Click **Insert**.
5. Configure the fields as required.
6. Click **Insert**.
7. Click **Apply**.

Energy Saver Schedules Field Descriptions

Name	Description
ScheduleDay	Specifies the day on which Energy Saver is activated or deactivated. The options are: • **monday** • **tuesday** • **wednesday** • **thursday** • **friday**

Table continues…

Name	Description
	- **saturday** - **sunday** - **weekdays** - **weekend**
ScheduleHour	Specifies the hour at which Energy Saver is activated or deactivated. The range is 0 to 23. **Note:** 0 is equivalent to 12 a.m., and 12 is equivalent to 12 p.m.
ScheduleMinute	Specifies the minute at which Energy Saver is activated or deactivated. The range is 0 to 59.
ScheduleAction	Specifies if Energy Saver is activated or deactivated. The options are: - **activate** - **deactivate**

Enable Energy Saver or EEE on Ports

You can enable Energy Saver or EEE using the Energy Saver tab accessed by the Edit navigation path, or the Power Management navigation path. Use one of the following procedures to enable either Energy Saver or EEE on ports.

Enable Energy Saver or EEE on Ports

About this task

Perform this procedure to enable Energy Saver or EEE on one or more ports.

Procedure

1. On the Device Physical View tab, select one or more ports.
2. In the navigation pane, expand **Edit** > **Port**.
3. Select **General**.
4. Select the **Energy Saver** tab.
5. Enable either Energy Saver or EEE:
   - To enable Energy Saver, select **EnergySaverEnabled**.
   - To enable EEE, select **EnergySaverEEEEnable**.
6. Select **Apply**.

Energy Saver Field Descriptions

Use the data in the following table to use the Energy Saver tab.

Name	Description
Port	Specifies the port number.
EnergySaverEnabled	Configures whether Energy Saver is enabled on the specific port.
EnergySavedPoeStatus	Specifies the Energy Saver PoE status for the specific port.
EnergySaverEEEEnable	Configures whether EEE is enabled on the specific port.

Enable Energy Saver or EEE on Ports

About this task

Perform this procedure to enable Energy Saver or EEE on one or more ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Power Management**.
2. Select **Energy Saver**.
3. Select the **Ports** tab.
4. Enable either Energy Saver or EEE:
    - To enable Energy Saver, in the **EnergySaverEnabled** column, double-click the field associated with the specific ports, and then select **true**.
    - To enable EEE, in the **EnergySaverEEEEnable** column, double-click the field associated with the specific ports, and then select **true**.
5. Select **Apply**.

Energy Saver Field Descriptions

Use the data in the following table to use the Energy Saver tab.

Name	Description
Port	Specifies the port number.
EnergySaverEnabled	Configures whether Energy Saver is enabled on the specific port.
EnergySaverPoEStatus	Specifies Energy Saver PoE status for the specific port.
EnergySaverEEEEnable	Configures whether EEE is enabled on the specific port.

View Energy Savings

About this task

Perform this procedure to view the amount of switch capacity and PoE power being saved on the units.

Procedure

1. In the navigation pane, expand **Configuration** > **Power Management**.
2. Click **Energy Saver**.
3. Click the **Energy Savings** tab.

Energy Savings field descriptions

Name	Description
UnitIndex	Specifies the unit number.
UnitSavings(1/10 watts)	Specifies the amount of switch capacity power being saved on the specific unit.
PoeSavings(1/10 watts)	Specifies the amount of PoE power being saved on the specific unit.

Chapter 13: Licensing

Table 37: Licensing product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
License files signed using Extreme Networks signature.	VSP 4450 Series	VOSS 6.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.1.2
	VSP 8400 Series	VOSS 6.1.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50
Subscription-based licenses	VSP 4450 Series	Not Supported
	VSP 4900 Series	Not Supported
	VSP 7200 Series	Not Supported
	VSP 7400 Series	Not Supported
	VSP 8200 Series	Not Supported
	VSP 8400 Series	Not Supported
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.0.50

Licensing Fundamentals

Licensing allows switch operators to select the features that best suits their needs. This section provides conceptual information about licensing. Subsequent sections discuss how to acquire, install, and enable licenses.

New switches include a Factory Default License to use all features (excluding MACsec). You can configure all features, except MACsec, without restrictions and save the configuration. Evaluation periods differ depending on the platform.

The hardware platforms support different levels and types of licenses. Refer to the topics in this section for detailed licensing information for your specific device.

- Feature Licensing for the VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, and VSP 8000 Series on page 271
- Feature Licensing for VSP 8600 on page 273
- Port Licensing for the VSP 7200 Series on page 275
- Subscription Licensing for XA1400 Series on page 276

License files

The VSP 4000 Series switch supports two types of license files — .dat and .lic. License files with .dat and .lic extension were created using an older license generator and are considered legacy licenses. License files that have an .xml extension are created using a newer license generator and are considered newer license files.

Feature Licensing for the VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, and VSP 8000 Series

The VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series support a licensing model that includes Base Licenses and Premier Licenses. The Base License, which is included with the purchase of the switch, enables the basic networking capabilities of the device. You can purchase Premier Licenses separately to enable advanced features on the switch.

Licenses are tied to the switch Base MAC address. After you generate the license through the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding, you can install the license on the switch.

Important:

If you require a change to or regeneration of legacy licenses for the VSP 4000 Series, send your email request to datalicensing@extremenetworks.com.

Note:

Release 6.1.2 or later is required to support licenses generated through the Extreme Networks Support Portal.

Extreme Networks supports only a single host (system MAC address) for each license file. You cannot use the same license file on multiple hosts.

The software continues to support .xml licenses generated by Avaya.

The following sections detail the different categories of licenses.

Factory Default License

New switches include a 60-day Factory Default License to use all features (excluding MACsec). You can configure all features, except MACsec, without restrictions and save the configuration.

You cannot configure any new feature after the 60-day period, but the switch continues to run with the existing configured features. If you reboot the switch after the 60-day period, and a valid software license is not present, licensed features in the configuration are not loaded. You must install a valid license to enable licensed features.

Note:

The 60-day evaluation period is based on the switch System Up Time.

Trial License

Trial licenses allow users to test licensed features at any time. The following two types of Trial Licenses are available:

- Trial License that allows the use of all features excluding MACsec
- Trial License that allows the use of all features including MACsec

A Trial License is valid for 60 days. You can activate a Trial License once per switch.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 55 days, and then once daily for the last 5 days. If you reboot the switch after the 60-day period, and a valid software license is not present, the configuration does not load. You must install a valid license to enable licensed features.

Base License

A Base license gives customers the right to use Base software features on the switch.

Premier License

Premier Licenses enable advanced features not available in the Base License. The following table provides information on the Premier Licenses that the switch supports.

License type	Supported features
Premier License	• DvR Controller • DvR interfaces on more than 24 VRFs/Layer 3 VSNs on Leaf nodes **Note:** DvR Leaf functionality is part of the base software license and the software allows you to create DvR interfaces on Layer 3 VSNs on Leaf nodes. Because a Premier license is required to configure more than 24 VRFs, for deployments where DvR Controllers have more than 24 VRFs configured with DvR, then Leaf nodes only create the first 24 Layer 3 VSNs (VRFs) and no more, unless you install a Premier or Premier with MACsec license. • Extreme Integrated Application Hosting • Fabric Connect Layer 3 Virtual Services Networks (VSNs) • Greater than 16 BGP peers • Greater than 24 VRFs • VXLAN Gateway
Premier with MACsec License	• DvR Controller • DvR interfaces on more than 24 VRFs/Layer 3 VSNs on Leaf nodes

Table continues…

License type	Supported features
	Note: DvR Leaf functionality is part of the base software license and the software allows you to create DvR interfaces on Layer 3 VSNs on Leaf nodes. Because a Premier license is required to configure more than 24 VRFs, for deployments where DvR Controllers have more than 24 VRFs configured with DvR, then Leaf nodes only create the first 24 Layer 3 VSNs (VRFs) and no more, unless you install a Premier or Premier with MACsec license. • Extreme Integrated Application Hosting • Fabric Connect Layer 3 Virtual Services Networks (VSNs) • Greater than 16 BGP peers • Greater than 24 VRFs • IEEE 802.1AE MACsec • VXLAN Gateway

License Types and Part Numbers

The following table lists the license types and the associated part numbers.

License Type	Part Number / Order Code
VSP 4000 Series and VSP 4900 Series Premier License	338836
VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series Premier License	380176
VSP 4000 Series and VSP 4900 Series Premier with MACsec License	338835
VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series Premier with MACsec License	380177
VSP 7400 Series Premier License	VSP-PRMR-LIC-P

Feature Licensing for VSP 8600

The VSP 8600 Series supports a licensing model that has two main categories of licenses: Base License and Feature Pack Licenses. A Base License enables base software features and one is required per IOC in the chassis. You require a Feature Pack License to enable additional features that are grouped into Feature Packs. These licenses are optional.

Licenses are tied to the switch Base MAC address. After you generate the license through Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding, you can install the license on the switch.

Note:

Release 6.1 is required to support licenses generated through the Extreme Networks Support Portal.

Important:

The software continues to support .xml licenses generated by Avaya.

The following sections detail the different categories of licenses supported on the VSP 8600 Series switch.

Factory Default License

New switches include a 30-day Factory Default License that allows you to use all features, excluding MACsec. You can configure all features, except MACsec, without restrictions and save the configuration.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 25 days, and then once daily for the last 5 days. If you reboot the switch after the 30-day period, and a valid software license is not present, the licensed features in the configuration are not loaded. You must install a valid license to enable the licensed features.

Trial License

Trial Licenses allow you to test the licensed features at any time. The following two types of Trial Licenses are available:

- Trial License that allows the use of all features excluding MACsec
- Trial License that allows the use of all features including MACsec

A Trial License is valid for 60 days. You can activate a Trial License once per switch.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 55 days, and then once daily for the last 5 days. If you reboot the switch after the 60-day period, and a valid software license is not present, the licensed features in the configuration are not loaded. You must install a valid license to enable the licensed features.

Base License

A Base License allows you to use the Base software features on the switch. A Base License is required for each IOC module that you plan to install in the chassis. If the number of IOCs exceeds the licensed IOC quantity, the ports on the excess IOCs are license-locked and appear administratively down.

The software validates the number of license entitlements against the IOC modules present and assigns the licenses sequentially to the I/O slots, starting from slot 1 to slot 8. For example, if you install modules in I/O slots 1 through 4 but only purchase three Base Licenses, the switch automatically assigns the licenses to slots 1 to 3. The ports on the module in slot 4 are in the license-locked state and appear administratively down because the license entitlements on the switch are only for 3 IOCs. If you would like to override the default entitlement assignment, you can reassign it to a different slot by using the `license-grant` command.

Feature Pack Licenses

Features that are not available in the Base License are grouped into Feature Packs based on use case. You require a license to use a Feature Pack. A Feature Pack License applies to the entire chassis; you do not need to purchase this license type for each installed IOC module. Feature Pack Licenses are optional, incremental to the Base License and sold separately.

The following table provides information on the Feature Pack licenses that the VSP 8600 Series supports.

License type	Supported features
Layer 3 Virtualization	• Fabric Connect Layer 3 Virtual Services Networks (VSNs) • DVR Controller • Greater than 25 VRFs • Greater than 17 BGP Peers
Layer 3 Virtualization with MACsec	• Fabric Connect Layer 3 Virtual Services Networks (VSNs) • DVR Controller • Greater than 25 VRFs • Greater than 17 BGP Peers • MACsec

VSP 8600 License types and part numbers

The following table provides the part numbers for the various licenses the VSP 8600 supports.

Table 38: Supported licenses

License type	Part number/ Order code
Base License - one per IOC Module	392259
Layer 3 Virtualization Feature Pack License - one per chassis	392670
Layer 3 Virtualization+MACsec Feature Pack License - one per chassis	392671

Port Licensing for the VSP 7200 Series

The VSP 7200 Series hardware models are available with twenty four 1/10 GbE SFP/SFP+ and four 40 GbE QSFP+ ports enabled by default. You must purchase a Port License to enable the remaining ports on the switch. You can use the Port License alone or combined with a Premier License or Premier License with MACsec at any time. When combining these licenses, the old license file must be deleted and the new license file that has the combination of Port and Premier or Premier with MACsec must be installed and loaded on the switch.

See Feature Licensing for the VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, and VSP 8000 Series on page 271 for more information about Premier License features.

The Port License order code is 386914.

Note:

Port Licenses are not available with Trial Licenses.

Subscription Licensing for XA1400 Series

Each XA1400 Series device requires a subscription license.

Licenses are tied to the switch Base MAC address and switch model type. After you generate the license through Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding, you can install the license on the switch.

Note:

VOSS Release 8.0.50 or later is required to support subscription licenses generated through the Extreme Networks Support Portal.

The following sections detail the different categories of licenses supported on the XA1400 Series switch.

Factory Default Trial License

A new switch includes a 60-day Factory Default Trial License starting from the time the switch is first booted. You can configure all features (except MACsec), without restrictions and save the configuration. No license file is required.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 55 days, and then once daily for the last 5 days. If you reboot the switch after the 60-day period, and a valid software license is not present, the licensed features in the configuration are not loaded. You must install a valid license to enable the licensed features.

Subscription License

All subscription licenses support all VOSS features on the switch, plus software upgrades and technical support services entitlement during the license term. A one, three, or five year subscription license is required for each XA1400 Series device. Three services entitlement tiers of license are available: ExtremeWorks, PartnerWorks, and ExtremeWorks Premier.

A Subscription License is available in two bandwidth tiers of licenses: Small License and Medium License. A Small License enables up to 100 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity, and a Medium License enables up to 500 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity.

License expiry notifications are sent to the console and management station every 30 days until the last 30 days of the subscription. Then every 5 days until the last 9 days of the subscription, and then daily until the Subscription License expires.

When a subscription expires, notification messages are shown on the console and in the alarms database, indicating that the license is expired. Existing software functionality is not impaired upon subscription license expiry. However, software upgrades are disallowed until the new license is activated. Additionally, access to Software and Services GTAC support is suspended for the product until a valid license is activated.

XA1400 Series License Types and Part Numbers

The following table provides the part numbers for the various licenses the XA1400 Series supports.

Table 39: Supported licenses

Small Subscription Licenses (up to 100 Mbps)	Part number/ Order code
1 year, ExtremeWorks	FCVPN-100-EW-1Y
1 year, PartnerWorks	FCVPN-100-PW-1Y
1 year, ExtremeWorks Premier	FCVPN-100-EWP-1Y
3 years, ExtremeWorks	FCVPN-100-EW-3Y
3 years, PartnerWorks	FCVPN-100-PW-3Y
3 years, ExtremeWorks Premier	FCVPN-100-EWP-3Y
5 years, ExtremeWorks	FCVPN-100-EW-5Y
5 years, PartnerWorks	FCVPN-100-PW-5Y
5 years, ExtremeWorks Premier	FCVPN-100-EWP-5Y

Medium Subscription Licenses (up to 500 Mbps)	Part number/ Order code
1 year, ExtremeWorks	FCVPN-500-EW-1Y
1 year, PartnerWorks	FCVPN-500-PW-1Y
1 year, ExtremeWorks Premier	FCVPN-500-EWP-1Y
3 years, ExtremeWorks	FCVPN-500-EW-3Y
3 years, PartnerWorks	FCVPN-500-PW-3Y
3 years, ExtremeWorks Premier	FCVPN-500-EWP-3Y
5 years, ExtremeWorks	FCVPN-500-EW-5Y
5 years, PartnerWorks	FCVPN-500-PW-5Y
5 years, ExtremeWorks Premier	FCVPN-500-EWP-5Y

Note:

500 Mbps Subscription Licenses are only supported on XA1480 devices.

License Installation using CLI

Install and manage a license file for the switch by using the Command Line Interface (CLI).

Note:

This section applies to multiple platforms. The command syntax and example outputs may not be identical on all hardware platforms.

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.

You can use the same procedure to load legacy license files, license.dat, on a VSP 4000 Series switch.

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 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. Load the license:

   ```
   load-license WORD<0-63>
   ```

   Note:

   If filename parameter is not used and 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 L3VWithMACsec.xml  /intflash/L3VWithMACsec.xml
local: L3VWithMACsec.xml remote: /intflash/L3VWithMACsec.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 L3VWithMACsec.xml
Switch:1(config)#CP1 [06/12/15 15:59:57.636:UTC] 0x000005bc 00000000 GlobalRouter SW INFO
License Successfully Loaded From </intflash/L3VWithMACsec.xml> License Type -- L3V with
MACsec
```

The following example shows an unsuccessful operation.

```
Switch:1(config)#load-license license_Switch_example.xml
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

The following table defines parameters for 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.

The following table defines parameters for the **load-license** command.

Variable	Value
WORD<0–63> **Note:** Exception: only supported on VSP 8600 Series.	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

Showing a License File

Display the existing software licenses on your device. If the switch uses a Trial License, the output shows the time remaining in the trial period.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Show the existing software licenses on your device:

   `show license`

Example

The following output shows a system with time remaining on a Trial License:

```
Switch:1>show license
License Type                     : TRIAL
LicenseTrialPeriodRemainingDays  : 59

************************************************************************
Features requiring a Premier license:
        -  Layer 3 VSNs
        -  MACsec
        -  Distributed Virtual Routing(DvR) Controller
        -  VXLAN GATEWAY
        -  >24 VRFs
        -  >16 BGP Peers
        -  Insight Virtualization
```

The following output is for a VSP 4000 Series switch that uses legacy .dat licenses. The output for the **`show license`** command for legacy licenses shows 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
        -  Distributed Virtual Routing(DvR) Controller
        -  >24 VRFs
```

The output for the **`show license`** command for .xml licenses shows 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 (includes Base features)
        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
        -  Distributed Virtual Routing(DvR) Controller
        -  VXLAN GATEWAY
        -  >24 VRFs
        -  >16 BGP Peers
```

The following **`show license`** command output is from a platform that supports Base Licenses per IO slot and Feature Pack Licenses.

```
Switch:1>show license

        License file name       :    /intflash/.sys/Base.xml
        License Type            :    BASE
        Duration Type           :    Perpetual
        Generation Time         :    2017/01/05 20:57:22
        Expiration Time         :
        Host ID                 :    F873A2045000
************************************************************************
Features requiring a L3V + MacSec license:
        -  Layer 3 VSNs
        -  MACsec
************************************************************************

        Number of IO license entitlements: 8
        License granted for slots        : 1  2  5  8

************************************************************************
```

The following **`show license`** command output is from a XA1400 Series platform that supports Subscription Licenses.

```
Switch:1>show license

 License file name      :    FCVPN500-EW-5YR.xml
        License Type            :    FCVPN500-EW-5YR
        Duration Type           :    TimeBased
        Generation Time         :    2019/06/10 06:50:08
        Expiration Time         :    2024/06/08
        Host ID                 :    DCB808B66000
************************************************************************
```

Assigning a Base License to an IOC module slot

About this task

The system validates the number of license entitlements against the IOC modules present and assigns the licenses sequentially to the I/O slots, starting from slot 1 to slot 8.

If you install a module in a slot that has a license assigned and later, when the module is moved to another slot that does not have a license assigned, you can reassign the license to the new slot by using the **`license-grant`** command.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Load the license on the slot and enable the ports on the IOC module:

   ```
   license-grant slot {slot[-slot][,...]}
   ```

3. Release the license from a slot:

   ```
   no license-grant slot {slot[-slot][,...]}
   ```

Example

Load the license on the specified slot and enable the ports on the IOC module:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#license-grant slot 2
License granted for slot: 2
Switch:1(config)#
```

License Installation using EDM

Install and manage a license file for the switch by using Enterprise Device Manager (EDM).

Note:

This section applies to multiple platforms. The fields may not be identical on all hardware platforms.

Install 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. 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

Note:

You can use the same procedure to load legacy license files, license.dat, on a VSP 4000 Series switch.

IPv4 and IPv6 addresses are supported.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Copy File** tab.
4. In the **Source** box, type the IP address of the file server where the license file is located and the name of the license file.
5. In the **Destination** box, type the flash device and the name of the license file.

   The license file name must 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 **Configuration** > **Edit**.
9. Click **Chassis**.
10. Click the **System** tab.
11. In **ActionGroup1**, select **loadLicense**.
12. In **LicenseFileName** box, type the name of the license file.
13. Click **Apply**.

    Important:

    If the loading fails, the switch cannot unlock the licensed features and reverts to base functionality.

14. On the **System** tab, in **ActionGroup1**, select **saveRuntimeConfig**.
15. Click **Apply**.

Copy File Field Descriptions

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

Name	Description
Source	Identifies the device and file name to copy. You must specify the full path and filename, for example, `<deviceip-ftp server>:/<filename>`
Destination	Identifies the location to which to copy the source file with the filename, for example, `/intflash/<filename>`
Action	Starts or stops the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

View License File Information

About this task

View information about the license file for the switch.

Procedure

1. In the navigation pane, expand **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.

Table continues…

Name	Description
	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.
RemainingDays	Indicates the days left before the factory default trial period or subscription license expires. **Note:** 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.

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.
VirtualIpAddr	Configures the virtual IP address that the primary CPU advertises and stores in the switch configuration file.
VirtualNetMask	Configures the net mask of the virtual management IP address.
VirtualIpv6Addr	Specifies the virtual IPv6 address.
VirtualIpv6PrefixLength	Specifies the length of the virtual IPv6 address prefix (in bits).

Table continues…

Name	Description
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
LicenseFileName + **Note:** Exception: only supported on the XA1400 Series and the VSP 8600 Series.	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
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
ActionGroup4	Can be the following action: • softReset—resets the device without running power-on tests • cpuSwitchOver—switches over to the other CPU • softResetCoreDump —reset with coredump
Result	Displays a message after you click **Apply**.

Table continues…

Name	Description
LocatorLED ✱ **Note:** Exception: only supported on VSP 4900 Series.	Configures the system Locator LED on or off. The default is off.

Assign a Base License to an IOC Module Slot

About this task

The system validates the number of license entitlements against the IOC modules present and assigns the licenses sequentially to the I/O slots, starting from slot 1 to slot 8.

If you install a module in a slot that has a license assigned and later, when the module is moved to another slot that does not have a license assigned, you can reassign the license to the new slot.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **License Grant** tab.
4. Do any one of the following:
   - To assign a license to a slot, double-click the cell in the **SlotGrant** column, and change the value to true.
   - To release a license from a slot, double-click the cell in the **SlotGrant** column and then change the value to false.
5. Click **Apply**.

License Grant field descriptions

Use the data in the following table to use the **License Grant** tab.

Name	Description
Slot	Specifies the IO slot number. Valid slots are 1 to 8.
SlotGrant	Specifies the license status on the IO slot. • **True** if valid license is granted to the slot • **False** if license is not granted to the slot

Chapter 14: Link Layer Discovery Protocol

Table 40: Link Layer Discovery Protocol product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Industry Standard Discovery Protocol (ISDP) (CDP compatible)	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
Link Layer Discovery Protocol (LLDP)	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.0.50
Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	Not Supported
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0
	XA1400 Series	VOSS 8.0.50

The following sections describe how to use Link Layer Discovery Protocol (LLDP) and Industry Standard Discovery Protocol (ISDP).

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.

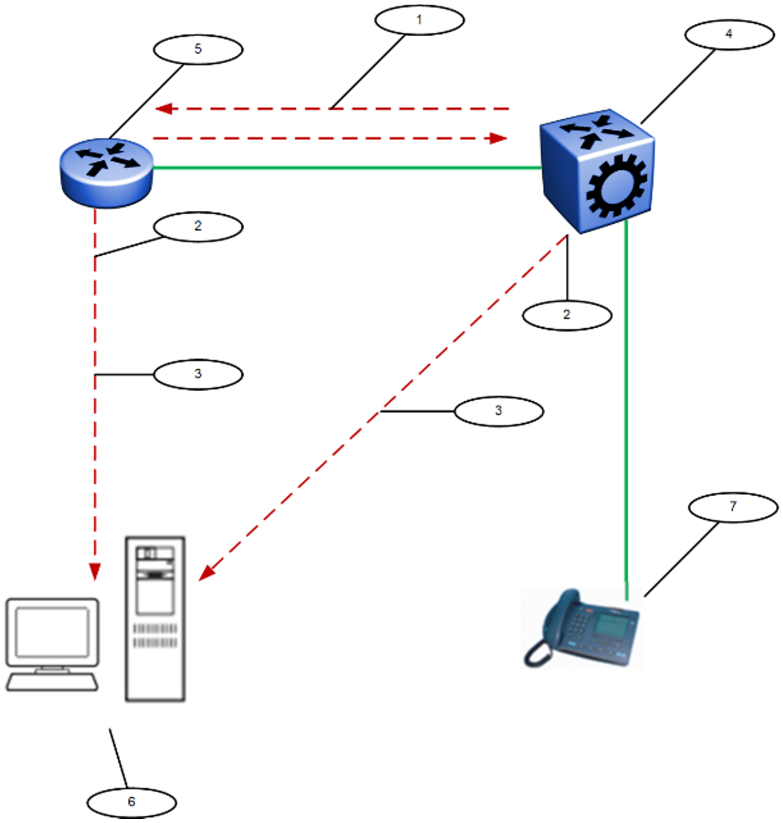


Figure 2: LLDP in a LAN

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.

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.

LLDP for the Segmented Management Instance

LLDP and SONMP both advertise the same topology IP address for the Segmented Management Instance management interface. LLDP supports IPv4 and IPv6 advertisement. If all three management interfaces are configured, the advertised default topology IP priority is management CLIP, then management VLAN, then management OOB. You can change the default topology IP using CLI or EDM. If multiple IPv4 addresses are configured on an OOB or VLAN management interface, the advertised IP priority is static IP address, then DHCP IP address, then link-local IP address.

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-Media Endpoint Discovery

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) defined in ANSI/TIA-1057, is an extension to the LLDP standard protocol as defined in IEEE 802.1AB. LLDP-MED provides support to deploy Voice over Internet Protocol (VoIP) telephones into the LAN environment. LLDP-MED provides additional TLVs for basic configuration, network policy configuration, location identification, and inventory management.

Following are the types of LLDP-MED devices:

- Network connectivity devices: provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. The LLDP-MED Network Connectivity device is a LAN access device based on:
    - LAN Switch or Router
    - IEEE 802.1 Bridge
    - IEEE 802.3 Repeater
    - IEEE 802.11 Wireless Access Point
    - Any device that supports the IEEE 802.1AB, LLDP-MED, and can relay IEEE 802 frames.

- Endpoint devices: located at the IEEE 802 LAN network edge, participating in the IP communication service using the LLDP-MED framework. The endpoint devices are divided into three classes:
  - Class 1 - LLDP-MED Generic Endpoint devices, for example, IP communication controllers.
  - Class 2 - LLDP-MED Media Endpoint devices, for example, media servers, conference bridges.
  - Class 3 - LLDP-MED Communication Endpoint devices, for example, IP telephones.

Organizational-specific TLVs for LLDP-MED

The organizational-specific TLVs for use by LLDP-MED network connectivity and endpoint devices are:

- Capabilities TLV — enables a network element to determine whether particular connected devices support LLDP-MED, and also discover the TLVs supported by specific network connectivity or endpoint devices.
- Network Policy Discovery TLV — enables both network connectivity and endpoint devices to advertise VLAN information, Layer 2, and Layer 3 priorities associated with a specific set of applications on a port. In addition, an LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.
- Location Identification Discovery TLV — allows network connectivity devices to advertise the appropriate location information for communication endpoint devices, including emergency call service location, to use in the context of location-based applications.
- Extended Power-via-MDI Discovery TLV — enables advanced power management between an LLDP-MED network connectivity and endpoint devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for network connectivity and endpoint devices.

  Important:

  Product notice: This TLV is not applicable on the VSP 8600 Series because Power over Ethernet (PoE) is not supported.
- Inventory Management Discovery TLV — enables tracking and identification of inventory-related attributes for endpoint devices. For example, manufacturer, model name, and software version.

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 the 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

The following table defines parameters for 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 the 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

The following table defines parameters for 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 the 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

To configure the switch as CDP-compatible, you must enable the Industry Standard Discovery Protocol (ISDP) on a port, or ports, on the switch. To enable ISDP, you use the **`lldp cdp`** command.

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 the 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. **(Optional)** 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
```

View 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. Display LLDP local system data:

```
show lldp local-sys-data [med]
```

3. Display the LLDP neighbor system information:

   ```
   show lldp neighbor [summary] [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

4. Display the list of ports:

   ```
   show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

5. Display the LLDP reception statistics:

   ```
   show lldp rx-stats [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

6. Display the LLDP statistics:

   ```
   show lldp stats
   ```

7. Display the LLDP transmission statistics:

   ```
   show lldp 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 : VSP-4450GSX-PWR+ (6.0.1.0)  BoxType: VSP-4450
               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: VSP8404 - Gbic1000BaseT Port 1/28
                SysDescr : VSP8404 (4.5.0.0)
                Address  : 192.0.2.47
--------------------------------------------------------------------------------

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 neighbor summary of all ports on the switch. You can also view this on a specific port.

```
Switch:1#show lldp neighbor summary

========================================================================================================================
                                                 LLDP Neighbor Summary
========================================================================================================================
LOCAL            IP              CHASSIS            REMOTE
PORT       PROT  ADDR            ID                 PORT               SYSNAME       SYSDESCR
------------------------------------------------------------------------------------------------------------------------
1/4        LLDP  0.0.0.0          f8:15:47:e1:dd:00  f8:15:47:e1:dd:06  VSP-4450GSX-~ VSP-4450GSX-PWR+ (6.0.1.0)
1/12       LLDP  192.0.2.77     a4:25:1b:53:6c:00  a4:25:1b:53:6c:28  VSP-7254XTQ   VSP-7254XTQ (6.0.0.0)
1/13       LLDP  192.0.2.34     00:14:0d:e3:40:00  00:14:0d:e3:40:c1  ERS-8606      ERS-8606 (7.2.10.1)
1/14       LLDP  192.0.2.78     a4:25:1b:52:34:00  a4:25:1b:52:34:28  VSP-7254XSQ   VSP-7254XSQ (6.0.0.0)
1/24       LLDP  192.0.2.94     00:13:65:a3:8c:00  00:13:65:a3:8c:18                Ethernet Routing Switch 5520-~
1/25       CDP   192.0.2.89     --                 FastEthernet2/0/5  cisco3750.Tr~ cisco WS-C3750-48P running on~
1/27       CDP   0.0.0.0          --                 FastEthernet3/0/6  Switch        cisco WS-C3750-48TS running o~
1/48       LLDP  192.0.2.76     b0:ad:aa:4e:dc:00  b0:ad:aa:4e:dc:68  VSP-8404      VSP-8404 (6.0.0.0)
------------------------------------------------------------------------------------------------------------------------
Total Neighbors : 8
```

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
...
...
```

Display LLDP-MED local system data:

```
Switch:1#show lldp local-sys-data med
=====================================================================================
                             LLDP Local System Data
=====================================================================================

               ChassisId: MAC Address        d4:78:56:f1:65:00
               SysName  : VSP-4450GSX-PWR+
               SysDescr : VSP-4450GSX-PWR+ (w.x.y.z)
               SysCap   : Br / Br

        MED Capabilities:       CNLSI
        MED Device Type:        Network Connectivity Device
        MED Power Device Type:  PSE Device
        HWRev: 03               FWRev: VU-Boot 2012.04-00034-g57194a8
        SWRev: v5.7.3.005       SerialNumber: 16JP1160E51D
        ManufName: Extreme Networks. ModelName: VSP-4450GSX-PWR+
        Asset ID: 16JP1160E51D

-------------------------------------------------------------------------------------

Port: 1/1

  MED Enabled Capabilities: CNLI
  MED Network Policy:
    Application Type: Voice
      VLAN ID: 412
      L2 Priority: 3
      DSCP Value: 57
      Tagging: Tagged Vlan
      Policy defined
    Application Type: Voice-Signaling
      VLAN ID: 7
      L2 Priority: 6
      DSCP Value: 24
      Tagging: Tagged Vlan
      Policy defined
  MED Location - Coordinate-based LCI:
    Latitude:  +12.3 (degrees) North
    Longitude: +42   (degrees) East
    Altitude:  +45   (meters)
    Datum: World Geodesic System (WGS84)
  MED Location - Civic Address LCI:
    Country code: RO
    Country: Romania
    City: Bucuresti
    Block: 12
    Street: Calea Floreasca
    Floor: 3
  MED Location - Emergency Call Service ELIN:
    ECS ELIN: 121416182022
  MED Extended Power via MDI:
    Power Value: 16.0 Watt
    Power Type: PSE
    Power Source: Primary
    Power Priority: Low

--------------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
MED Capabilities Legend: (Supported/Enabled)
  C= Capabilities, N= Network Policy; L= Location Identification;
  I= Inventory; S= Extended Power via MDI - PSE; D= Extended Power via MDI - PD.
```

Variable Definitions

The following table defines parameters for the **show lldp** command.

Variable	Value
local-sys-data	Displays the LLDP local system data.
neighbor [summary] [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 the 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 the 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.

Table continues…

Variable	Value
	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 the 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 the platform supports channelization and the port is 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]] [,...]}] | [summary {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] [med]}
   ```

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  : 192.0.2.98
                SysDescr : Ethernet Routing Switch 5650TD-PWR  HW:E.10 FW:6.0.0.18 
SW:v6.6.3.015
--------------------------------------------------------------------------------------------
-------
Total Neighbors : 1
--------------------------------------------------------------------------------------------
-------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

```
Switch:1#show lldp neighbor summary

==========================================================================================================
                                                 LLDP Neighbor Summary
==========================================================================================================
LOCAL           IP              CHASSIS            REMOTE
PORT       PROT  ADDR            ID                 PORT               SYSNAME       SYSDESCR
----------------------------------------------------------------------------------------------------------
1/4        LLDP  0.0.0.0         f8:15:47:e1:dd:00  f8:15:47:e1:dd:06  VSP-4450GSX-~ VSP-4450GSX-PWR+ (6.0.1.0)
1/12       LLDP  192.0.2.77     a4:25:1b:53:6c:00  a4:25:1b:53:6c:28  VSP-7254XTQ   VSP-7254XTQ (6.0.0.0)
1/13       LLDP  192.0.2.34     00:14:0d:e3:40:00  00:14:0d:e3:40:c1  ERS-8606      ERS-8606 (7.2.10.1)
1/14       LLDP  192.0.2.78     a4:25:1b:52:34:00  a4:25:1b:52:34:28  VSP-7254XSQ   VSP-7254XSQ (6.0.0.0)
1/24       LLDP  192.0.2.94    00:13:65:a3:8c:00  00:13:65:a3:8c:18                Ethernet Routing Switch 5520-~
1/25       CDP   192.0.2.89     --                FastEthernet2/0/5  cisco3750.Tr~ cisco WS-C3750-48P running on~
1/27       CDP   0.0.0.0         --                FastEthernet3/0/6  Switch        cisco WS-C3750-48TS running o~
1/48       LLDP  192.0.2.76     b0:ad:aa:4e:dc:00  b0:ad:aa:4e:dc:68  VSP-8404      VSP-8404 (6.0.0.0)
----------------------------------------------------------------------------------------------------------
Total Neighbors : 8
```

```
Switch:1#show lldp neighbor  med

==========================================================================================
                                    LLDP Neighbor MED
==========================================================================================

Port: 1/5       Index    : 1
                Protocol : LLDP
                ChassisId: MAC Address        00:19:e1:4e:9c:00
                PortId   : MAC Address        00:19:e1:4e:9c:08
                SysName  :
                SysCap   : Br / Br
                PortDescr: Port 8
                SysDescr : Ethernet Routing Switch 5650TD-PWR    HW:E.10     FW:6.0.0.18 
SW:v6.6.3.015
                Address  : 10.101.124.254

Port: 1/12      Index    : 2
                Protocol : LLDP
                ChassisId: Network Address    1.192.168.170
                PortId   : MAC Address        cc:f9:54:a4:6e:a0
                SysName  : AVXA46EA0
                SysCap   : BT / B
                PortDescr:
                SysDescr :
                Address  : 192.168.170.108

  MED Capabilities supported: CNI
  MED Capabilities enabled: CNI
    Device Type: Endpoint Class 3
  MED Inventory (I):
    Hardware Revision:  9611GD01A
    Firmware Revision:  S96x1_UKR_V30r3350_V30r3350.tar
    Software Revision:  S96x1_SALBR7_0_0r39_V4r83.tar
    Serial Number:      11WZ273508WM
    Manufacturer Name:  Avaya
    Model Name:         9611G
  MED Network Policy (N):
    Application Type: Voice
```

```
      VLAN ID: 0
      L2 Priority: 6
      DSCP Value: 46
      Tagging: Untagged Vlan
      Policy Defined
    Application Type: Voice Signaling
      VLAN ID: 0
      L2 Priority: 6
      DSCP Value: 34
      Tagging: Untagged Vlan
      Policy Defined
------------------------------------------------------------------------------------------
Total Neighbors : 2
------------------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
------------------------------------------------------------------------------------------
MED Capabilities Legend: (Supported/Enabled)
C= MED Capabilities,  N= Network Policy,  L= Location Identification,
I= Inventory,  S= Extended Power via MDI - PSE,  D= Extended Power via MDI - PD.
------------------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for 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 slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
med	Displays LLDP neighbors learned based on LLDP-MED TLV information.
summary *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Displays the summary of LLDP neighbors 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 the 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
```

LLDP-MED Configuration Using CLI

Configure LLDP-MED information for local and remote systems on specific ports. LLDP-MED is enabled by default and all its TLVs are enabled for transmission.

To configure LLDP-MED TLVs in the LLDP PDUs on an interface:

- Configure LLDP-MED.
- Configure LLDP-MED network policy and location information.
- The switch automatically configures LLDP-MED capabilities, power, and inventory information.

Configure LLDP-MED Network Policies on Ports

About this task

Perform this procedure to configure network policies on specific ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   Note:

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

2. Configure a network policy:

   ```
   lldp med-network-policies {guest-voice | guest-voice-signaling |
   softphone-voice | streaming-video | video-conferencing | video-
   ```

```
signaling | voice | voice-signaling} [dscp <0-63>] [priority <0-7>]
[tagging {tagged|untagged}] [vlan-id <0-4059>]
```

Example

Configuring guest voice network policy on port 1/2:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitEthernet 1/2
Switch:1(config-if)#lldp med-network-policies guest-voice dscp 1 priority 5 tagging
tagged vlan-id 5
```

Variable Definitions

The following table defines parameters for the **`lldp med-network-policies`** command.

Variable	Value
{guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling}	Specifies the type of network policy.
dscp *<0-63>*	Specifies the Layer 3 DiffServ Code Point (DSCP) value, as defined in IETF RFC 2474 and RFC 2475. The default is 0.
priority *<0-7>*	Specifies the priority level, as defined in IEEE 802.1D. The default is 0.
tagging *{tagged* | *untagged}*	Specifies the type of VLAN tagging to apply on the selected ports. The default is untagged.
vlan-id *<0-4059>*	Specifies the VLAN ID for the port, as defined in IEEE 802.1Q. If you configure priority tagged frames, the system recognizes only the 802.1D priority level and uses a value of 0 for the VLAN ID of the ingress port. The default is 0.

Configure LLDP-MED Civic Address Location Information

About this task

Perform the following procedure to configure civic address location information of local LLDP-MED on specific ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

Note:

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

2. Configure the civic address location by configuring the country-code and at least one other location parameter:

   ```
   lldp location-identification civic-address country-code WORD<2-2>
   (additional-code additional-information apartment block building
   city city-district county floor house-number house-number-suffix
   landmark leading-street-direction name place-type pobox postal-
   community-name postal-zip-code room-number state street street-
   suffix trailing-street-suffix) WORD<0-255>
   ```

   Note:

   If you try to configure a civic-address with a large number of arguments, 26 or more, the command fails and a software message informs you to split the command into multiple smaller commands.

Example

Configuring civic address location on port 2/12:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitEthernet 2/12
Switch:1(config-if)#lldp location-identification civic-address country-code US city New
York
```

Variable Definitions

The following table defines parameters for the **`lldp location-identification civic-address`** command.

Variable	Value
additional-code WORD<0–255>	Specifies the location information parameters.
additional-information WORD<0–255>	Example: South Wing
apartment WORD<0–255>	Example: Apt 42
block WORD<0–255>	Specifies a block, e.g. 3
building WORD<0–255>	Example: Low Library
city WORD<0–255>	Specifies a city, e.g. Sunnyvale
city-district WORD<0–255>	Specifies a city district, e.g. Santa Clara
country-code WORD<2–2>	Specifies a country using a 2 character string, example US (United States), CA (Canada).
county WORD<0–255>	Specifies a county, e.g. Alameda
floor WORD<0–255>	Example: 8
house-number WORD<0–255>	Specifies a house number, e.g. 123

Table continues…

Variable	Value
house-number-suffix WORD<0–255>	Specifies a house number suffix, e.g. A, 1/2
landmark WORD<0–255>	Specifies a landmark, e.g. Columbia University
leading-street-direction WORD<0–255>	Specifies a leading street direction, e.g. N
name WORD<0–255>	Example: Joe's Barbershop
place-type WORD<0–255>	Example: office
pobox WORD<0–255>	Example: 12345
postal-community-name WORD<0–255>	Example: Leonia
postal-zip-code WORD<0–255>	Specifies a postal or zip code, e.g. 95054
room-number WORD<0–255>	Example: 450F
state WORD<0–255>	Specifies a state, e.g. NJ, FL
street WORD<0–255>	Specifies a street, e.g. Great America Parkway
street-suffix WORD<0–255>	Specifies a street suffix, e.g. Ave, Blvd
trailing-street-suffix WORD<0–255>	Specifies a trailing street suffix, e.g. SW

Configure LLDP-MED Coordinate Based Location Information

About this task

Perform the following procedure to configure coordinate based location information of local LLDP-MED on specific ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   Note:

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

2. Configure coordinate based location:

   ```
   lldp location-identification coordinate (altitude WORD<1-13> {floors
   | meters} datum {NAD83/MLLW | NAD83/NAVD88 | WGS84} latitude
   WORD<1-14> {NORTH | SOUTH} longitude WORD<1-14> {EAST | WEST})
   ```

Example

Configuring coordinate based location on port 1/2:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitEthernet 1/2
Switch:1(config-if)#lldp location-identification coordinate-base altitude 3 floors
```

Variable Definitions

The following table defines parameters for the **`lldp location-identification coordinate`** command.

Variable	Value
altitude *WORD<1–13>*	Specifies the value for altitude. The units of measurement are: • *floors* • *meters*
datum	Specifies the reference datum. The formats are: • NAD83/MLLW • NAD83/NAVD88 • WGS84
latitude *WORD<1-14>*	Specifies the latitude in degrees, and its relation to the equator from North or South.
longitude *WORD<1-14>*	Specifies the longitude in degrees, and its relation to the prime meridian from East or West.

Configure LLDP-MED Emergency Call Service Location

Perform the following procedure to configure emergency call service location of local LLDP-MED on specific ports.

About this task

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   Note:

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

2. Configure emergency call service location:

   ```
   lldp location-identification ecs-elin WORD<10-25>
   ```

Example

Configuring emergency call service location on port 2/1–2/10:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabitEthernet 2/1-2/10
Switch:1(config-if)#lldp location-identification ecs-elin 123456789
```

Variable Definitions

The following table defines parameters for the **`lldp location-identification ecs-elin`** command.

Variable	Value
WORD<10–25>	Specifies the emergency line information number for emergency call service.

Display Local LLDP-MEDLocation Information

About this task

Perform this procedure to display location information of the LLDP-MED configured locally.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display location information for local LLDP-MED:

   ```
   show lldp [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   location-identification
   ```

Example

```
Switch:1>enable
Switch:1#show lldp port 1/1-1/3 location-identification
======================================================================================
                              LLDP-MED Location Information
======================================================================================

Port: 1/1

  MED Location - Coordinate-based LCI:
    Latitude:  +12.3 (degrees) North
    Longitude: +42   (degrees) East
    Altitude:  +45   (meters)
    Datum: World Geodesic System (WGS84)
  MED Location - Civic Address LCI:
    Country code: RO
    Country: Romania
    City: Bucuresti
    Block: 12
```

```
    Street: Calea Floreasca
    Floor: 3
  MED Location - Emergency Call Service ELIN:
    ECS ELIN: 121416182022

Port: 1/2

    MED Location - Civic Address LCI:
    Country code: RO
    Country: Romania
    City: Bucuresti
    Block: 12
    Street: Calea Floreasca
    Floor: 3

Port: 1/3

  MED Location - Coordinate-based LCI:
    Latitude:  +12.3 (degrees) North
    Longitude: +42   (degrees) East
    Altitude:  +45   (meters)
    Datum: World Geodesic System (WGS84)
  MED Location - Emergency Call Service ELIN:
    ECS ELIN: 121416182022
```

Display LLDP-MED Local Network Policies Configuration

About this task

Perform this procedure to display LLDP-MED network policies locally configured on specific ports.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display LLDP-MED network policies configured:

   `show lldp [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}] med-network-policies [guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling]`

Example

```
Switch:1>enable
Switch:1#show lldp med-network-policies
==========================================================================================
                                LLDP-MED Network Policies
==========================================================================================
  Port       Application Type          VlanID    Tagging    DSCP    Priority
------------------------------------------------------------------------------------------
  1/2        Voice                     4         Untagged   0       0
  1/2        Guest Voice               0         Untagged   3       0
------------------------------------------------------------------------------------------
```

View 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. Display LLDP local system data:

   ```
   show lldp local-sys-data [med]
   ```

3. Display the LLDP neighbor system information:

   ```
   show lldp neighbor [summary] [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

4. Display the list of ports:

   ```
   show lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

5. Display the LLDP reception statistics:

   ```
   show lldp rx-stats [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

6. Display the LLDP statistics:

   ```
   show lldp stats
   ```

7. Display the LLDP transmission statistics:

   ```
   show lldp 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 : VSP-4450GSX-PWR+ (6.0.1.0)  BoxType: VSP-4450
               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: VSP8404 - Gbic1000BaseT Port 1/28
                SysDescr : VSP8404 (4.5.0.0)
                Address  : 192.0.2.47
-------------------------------------------------------------------------------

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 neighbor summary of all ports on the switch. You can also view this on a specific port.

```
Switch:1#show lldp neighbor summary

========================================================================================================================
                                                 LLDP Neighbor Summary
========================================================================================================================
LOCAL           IP              CHASSIS            REMOTE
PORT       PROT  ADDR            ID                 PORT               SYSNAME       SYSDESCR
------------------------------------------------------------------------------------------------------------------------
1/4        LLDP  0.0.0.0         f8:15:47:e1:dd:00  f8:15:47:e1:dd:06  VSP-4450GSX-~ VSP-4450GSX-PWR+ (6.0.1.0)
1/12       LLDP  192.0.2.77     a4:25:1b:53:6c:00  a4:25:1b:53:6c:28  VSP-7254XTQ   VSP-7254XTQ (6.0.0.0)
1/13       LLDP  192.0.2.34     00:14:0d:e3:40:00  00:14:0d:e3:40:c1  ERS-8606      ERS-8606 (7.2.10.1)
1/14       LLDP  192.0.2.78     a4:25:1b:52:34:00  a4:25:1b:52:34:28  VSP-7254XSQ   VSP-7254XSQ (6.0.0.0)
1/24       LLDP  192.0.2.94     00:13:65:a3:8c:00  00:13:65:a3:8c:18                Ethernet Routing Switch 5520-~
1/25       CDP   192.0.2.89     --                 FastEthernet2/0/5  cisco3750.Tr~ cisco WS-C3750-48P running on~
1/27       CDP   0.0.0.0         --                 FastEthernet3/0/6  Switch        cisco WS-C3750-48TS running o~
1/48       LLDP  192.0.2.76     b0:ad:aa:4e:dc:00  b0:ad:aa:4e:dc:68  VSP-8404      VSP-8404 (6.0.0.0)
------------------------------------------------------------------------------------------------------------------------
Total Neighbors : 8
```

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
...
...
```

Display LLDP-MED local system data:

```
Switch:1#show lldp local-sys-data med
======================================================================================
                             LLDP Local System Data
======================================================================================
               ChassisId: MAC Address        d4:78:56:f1:65:00
               SysName  : VSP-4450GSX-PWR+
               SysDescr : VSP-4450GSX-PWR+ (w.x.y.z)
               SysCap   : Br / Br

        MED Capabilities:       CNLSI
        MED Device Type:        Network Connectivity Device
        MED Power Device Type:  PSE Device
        HWRev: 03               FWRev: VU-Boot 2012.04-00034-g57194a8
        SWRev: v5.7.3.005       SerialNumber: 16JP1160E51D
        ManufName: Extreme Networks. ModelName: VSP-4450GSX-PWR+
        Asset ID: 16JP1160E51D

--------------------------------------------------------------------------------------

Port: 1/1

  MED Enabled Capabilities: CNLI
  MED Network Policy:
    Application Type: Voice
      VLAN ID: 412
      L2 Priority: 3
      DSCP Value: 57
      Tagging: Tagged Vlan
      Policy defined
    Application Type: Voice-Signaling
      VLAN ID: 7
      L2 Priority: 6
      DSCP Value: 24
      Tagging: Tagged Vlan
      Policy defined
  MED Location - Coordinate-based LCI:
    Latitude:  +12.3 (degrees) North
    Longitude: +42   (degrees) East
    Altitude:  +45   (meters)
    Datum: World Geodesic System (WGS84)
  MED Location - Civic Address LCI:
    Country code: RO
    Country: Romania
    City: Bucuresti
    Block: 12
    Street: Calea Floreasca
    Floor: 3
  MED Location - Emergency Call Service ELIN:
    ECS ELIN: 121416182022
  MED Extended Power via MDI:
    Power Value: 16.0 Watt
    Power Type: PSE
    Power Source: Primary
    Power Priority: Low

--------------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
MED Capabilities Legend: (Supported/Enabled)
  C= Capabilities, N= Network Policy; L= Location Identification;
  I= Inventory; S= Extended Power via MDI - PSE; D= Extended Power via MDI - PD.
```

Variable Definitions

The following table defines parameters for the **`show lldp`** command.

Variable	Value
local-sys-data	Displays the LLDP local system data.
neighbor [summary] [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 the 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.
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 the 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 the 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 the platform supports channelization and the port is 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]] [,...]}*] | [summary *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*] [med]}

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  : 192.0.2.98
                SysDescr : Ethernet Routing Switch 5650TD-PWR  HW:E.10 FW:6.0.0.18
SW:v6.6.3.015
------------------------------------------------------------------------------------------
-------
Total Neighbors : 1
------------------------------------------------------------------------------------------
-------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

```
Switch:1#show lldp neighbor summary

=========================================================================================================
                                                 LLDP Neighbor Summary
=========================================================================================================
LOCAL            IP              CHASSIS            REMOTE
PORT       PROT  ADDR            ID                 PORT              SYSNAME       SYSDESCR
---------------------------------------------------------------------------------------------------------
1/4        LLDP  0.0.0.0         f8:15:47:e1:dd:00  f8:15:47:e1:dd:06  VSP-4450GSX-~ VSP-4450GSX-PWR+ (6.0.1.0)
1/12       LLDP  192.0.2.77     a4:25:1b:53:6c:00  a4:25:1b:53:6c:28  VSP-7254XTQ   VSP-7254XTQ (6.0.0.0)
1/13       LLDP  192.0.2.34     00:14:0d:e3:40:00  00:14:0d:e3:40:c1  ERS-8606      ERS-8606 (7.2.10.1)
1/14       LLDP  192.0.2.78     a4:25:1b:52:34:00  a4:25:1b:52:34:28  VSP-7254XSQ   VSP-7254XSQ (6.0.0.0)
1/24       LLDP  192.0.2.94    00:13:65:a3:8c:00  00:13:65:a3:8c:18               Ethernet Routing Switch 5520-~
1/25       CDP   192.0.2.89     --                 FastEthernet2/0/5  cisco3750.Tr~ cisco WS-C3750-48P running on~
1/27       CDP   0.0.0.0         --                 FastEthernet3/0/6  Switch        cisco WS-C3750-48TS running o~
1/48       LLDP  192.0.2.76     b0:ad:aa:4e:dc:00  b0:ad:aa:4e:dc:68  VSP-8404      VSP-8404 (6.0.0.0)
---------------------------------------------------------------------------------------------------------
Total Neighbors : 8
```

```
Switch:1#show lldp neighbor  med

==========================================================================================
                                   LLDP Neighbor MED
==========================================================================================

Port: 1/5       Index    : 1
                Protocol : LLDP
                ChassisId: MAC Address        00:19:e1:4e:9c:00
                PortId   : MAC Address        00:19:e1:4e:9c:08
                SysName  :
                SysCap   : Br / Br
                PortDescr: Port 8
                SysDescr : Ethernet Routing Switch 5650TD-PWR    HW:E.10     FW:6.0.0.18
SW:v6.6.3.015
                Address  : 10.101.124.254

Port: 1/12      Index    : 2
                Protocol : LLDP
                ChassisId: Network Address    1.192.168.170
                PortId   : MAC Address        cc:f9:54:a4:6e:a0
                SysName  : AVXA46EA0
                SysCap   : BT / B
                PortDescr:
                SysDescr :
                Address  : 192.168.170.108

  MED Capabilities supported: CNI
  MED Capabilities enabled: CNI
    Device Type: Endpoint Class 3
  MED Inventory (I):
    Hardware Revision:  9611GD01A
    Firmware Revision:  S96x1_UKR_V30r3350_V30r3350.tar
    Software Revision:  S96x1_SALBR7_0_0r39_V4r83.tar
    Serial Number:      11WZ273508WM
    Manufacturer Name:  Avaya
    Model Name:         9611G
  MED Network Policy (N):
    Application Type: Voice
      VLAN ID: 0
      L2 Priority: 6
      DSCP Value: 46
      Tagging: Untagged Vlan
      Policy Defined
    Application Type: Voice Signaling
      VLAN ID: 0
      L2 Priority: 6
      DSCP Value: 34
      Tagging: Untagged Vlan
      Policy Defined
------------------------------------------------------------------------------------------
Total Neighbors : 2
------------------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
------------------------------------------------------------------------------------------
MED Capabilities Legend: (Supported/Enabled)
C= MED Capabilities,  N= Network Policy,  L= Location Identification,
I= Inventory,  S= Extended Power via MDI - PSE,  D= Extended Power via MDI - PD.
------------------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for 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 slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Table continues…

Variable	Value
med	Displays LLDP neighbors learned based on LLDP-MED TLV information.
summary *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Displays the summary of LLDP neighbors 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Link Layer Discovery Protocol configuration using EDM

This section describes how to configure LLDP on your switch using EDM.

Configure LLDP Global Information

Use this procedure to configure or view LLDP global information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. Click the **Globals** tab.
4. 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. 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.

Table continues…

Field	Description
	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.

View the LLDP Port Information

Use this procedure to view the LLDP port information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. Click the **Port** tab.
4. 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.
5. 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.
6. View the set of TLVs whose transmission using LLDP is always allowed by network management in the **TLVsTxEnable** field.
7. **(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**.

8. 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.
9. Click **Apply** to save any configuration changes.
10. 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. The default is an empty set of TLVs.
CdpAdminState	Specifies the CDP administrative status of the port. Configure this field to true to enable the Industry Standard Discovery Protocol (ISDP) on a port. ISDP is CDP-compatible. • true: indicates CDP is enabled. • false: indicates CDP is disabled.

Table continues…

Name	Description
	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.

View 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 **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. Click the **TX Stats** tab.

   The transmission statistics are displayed.
4. To view the transmission statistics graphically for a port:
   1. 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 use the TX Stats tab.

Name	Description
PortNum	Specifies the port number.
FramesTotal	Specifies the total number of LLDP frames transmitted.

View 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 **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. Click the **RX Stats** tab.
4. 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 use the RX Stats tab.

Name	Description
PortNum	Specifies the port number.
FramesDiscardedTotal	Specifies the number of LLDP frames received on the port, but discarded, for any reason.

Table continues…

Name	Description
	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.

View LLDP Local System Information

Use this procedure to view the LLDP local system information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. 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

Table continues…

Name	Description
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.

View LLDP Local Port Information

Use this procedure to view the LLDP local port information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **LLDP**.
3. 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.
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.

View LLDP Neighbor Information

Use this procedure to view the LLDP neighbor information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.

2. Click **LLDP**.
3. 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.
ProtocolType	Indicates whether the entry protocol is CDP or LLDP.
SysName	Indicates the name of the remote system.
IpAddress	Indicates the neighbor's IP address.
PortIdSubType	Indicates the type of encoding used to identify the remote port.
PortId	Indicates the remote port ID.
PortDesc	Indicates the remote port description.
ChassisIdSubtype	Indicates the type of encoding used to identify the remote system chassis. • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • 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.
SysDesc	Indicates the description of the remote system.

LLDP-MED Configuration Using EDM

Configure LLDP-MED information for local and remote systems on specific ports. LLDP-MED is enabled by default and all its TLVs are enabled for transmission.

To configure LLDP-MED TLVs in the LLDP PDUs on an interface:

- Configure LLDP-MED.

- Configure LLDP-MED location information.
- The switch automatically configures LLDP-MED capabilities, power, and inventory information.

View LLDP-MED Local Policy Information

About this task

Perform this procedure to view policy information for local LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Local Policy** tab.

Local Policy Field Descriptions

Name	Description
PortNum	Specifies the port.
PolicyAppType	Specifies the application type.
PolicyVlanId	Specifies the VLAN ID for the port, as defined in IEEE 802.1Q-2003. The value 0 is used if the device is using priority tagged frames, which means only the 802.1D priority level is significant, and the default VLAN ID of the ingress port is used instead.
PolicyPriority	Specifies the Layer 2 priority used for the specified application type, as defined in IEEE 802.1D-2004. The default is 0.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) associated with a specific port on the local LLDP-MED, as defined in IETF RFC 2474 and RFC 2475. The default is 0.
PolicyTagged	Specifies whether the application uses a tagged or untagged VLAN, as defined by IEEE 802.1Q-2003. • true — uses tagged VLAN • false — uses untagged VLAN or does not support a port-based VLAN

Add LLDP-MED Local Location Information

About this task

Perform this procedure to add location information of local LLDP-MED configured on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Local Location** tab.
4. In **LocationInfo** column, double-click on the cell, and type the information.

Local Location Field Descriptions

Name	Description
PortNum	Specifies the port number.
LocationSubtype	Specifies the location subtype of the local LLDP-MED: • coordinateBased • civicAddress • elin
LocationInfo	Specifies the location information of local LLDP-MED. The parsing of this information depends on the location subtype.

View LLDP-MED Local PoE PSE Information

About this task

Perform this procedure to view PoE Power Sourcing Entity (PSE) information for local LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Local PoE PSE** tab.

Local PoE PSE Field Descriptions

Name	Description
PortNum	Specifies the port.
PSEPortPowerAvailable	Specifies the value of the power available (in units of 0.1 watts) from the PSE through the specific port.

Table continues…

Name	Description
PSEPortPDPriority	Specifies the Power Device (PD) power priority for the PSE port (see RFC 3621): • unknown — priority is not configured or known by the PD • critical • high • low

View LLDP-MED Neighbor Capabilities Information

About this task

Perform this procedure to view capabilities information for remote LLDP-MED on specific ports based on the information advertised by the remote device and received on each port in the capabilities TLV.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor Capabilities** tab.

Neighbor Capabilities Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the connection instance unique to the remote LLDP-MED.
CapSupported	Specifies the LLDP-MED capabilities supported on the remote system.
CapCurrent	Specifies the LLDP-MED capabilities that are enabled on the remote system.
DeviceClass	Specifies the remote LLDP-MED device class.

View LLDP-MED Neighbor Policy Information

About this task

Perform this procedure to view policy information of remote LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor Policy** tab.

Neighbor Policy Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.
PolicyAppType	Specifies the policy application type.
PolicyVlanId	Specifies the VLAN ID for the port, as defined in IEEE 802.1Q-2003. The value 0 is used if the device is using priority tagged frames, which means only the 802.1D priority level is significant, and the default VLAN ID of the ingress port is used instead.
PolicyPriority	Specifies the Layer 2 priority used for the specified application type, as defined in IEEE 802.1D-2004. The default value is 0.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) associated with a specific port on the remote LLDP-MED, as defined in IETF RFC 2474 and RFC 2475. The default value is 0.
PolicyUnknown	Specifies the network policy for the remote LLDP-MED is currently unknown.
PolicyTagged	Specifies whether the application uses a tagged or untagged VLAN, as defined by IEEE 802.1Q-2003. • true — uses tagged VLAN • false — uses untagged VLAN or does not support a port based VLAN

View LLDP-MED Neighbor Location Information

About this task

Perform this procedure to view location information of remote LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor Location** tab.

Neighbor Location Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.
LocationSubType	Specifies the subtype of the remote LLDP-MED location: • coordinateBased • civicAddress • elin
LocationInfo	Specifies the location information of the remote LLDP-MED.

View LLDP-MED Neighbor PoE Information

About this task

Perform this procedure to view PoE information of remote LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor PoE** tab.

Neighbor PoE Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.
PoEDeviceType	Specifies the type of PoE LLDP-MED. • PseDevice: specifies the device as a Power Sourcing Entity (PSE). • pdDevice: specifies the device as a Power Device (PD). • none: specifies that the device does not support PoE.

View LLDP-MED Neighbor PoE PSE Information

About this task

Perform this procedure to view PoE Power Sourcing Entity (PSE) information for remote LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor PoE PSE** tab.

Neighbor PoE PSE Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.
PSEPowerAvailable	Specifies the power available from the PSE connected remotely to the specific port.

Table continues…

Name	Description
PSEPowerSource	Specifies the type of PSE Power Source for the remote LLDP-MED. • unknown • primary • backup
PSEPowerPriority	Specifies the power priority associated with the PSE LLDP-MED, for more information, see RFC 3621. • unknown • critical • high • low

View LLDP-MED Neighbor PoE PD Information

About this task

Perform this procedure to view PoE Powered Device (PD) information for remote LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor PoE PD** tab.

Neighbor PoE PD Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.
PDPowerReq	Specifies the value of the power required by a PD LLDP-MED connected remotely to the port.

Table continues…

Name	Description
PDPowerSource	Specifies the power source being utilized by the PD LLDP-MED. • from PSE: specifies that the device advertises its power source as received from a PSE. • local: specifies that the device advertises its power source as local. • local and PSE: specifies that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Specifies the priority of the PD LLDP-MED connected remotely to the port, for more information, see RFC 3621. • unknown — priority is not configured for the PD LLDP-MED • critical • high • low

View LLDP-MED Neighbor Inventory Information

About this task

Perform this procedure to view inventory attributes for LLDP-MED on specific ports.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Diagnostics** > **802_1ab**.
2. Click **Port MED**.
3. Click the **Neighbor Inventory** tab.

Neighbor Inventory Field Descriptions

Name	Description
TimeMark	Specifies the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Specifies the port on which the remote LLDP-MED information is received.
Index	Specifies the particular connection instance that is unique to the remote LLDP-MED.

Table continues…

Name	Description
HardwareRev	Specifies the current hardware revision of the LLDP-MED.
FirmwareRev	Specifies the current firmware revision of the LLDP-MED.
SoftwareRev	Specifies the current software revision of the LLDP-MED.
SerialNum	Specifies the current serial number of the LLDP-MED.
MfgName	Specifies the manufacturer of the LLDP-MED.
ModelName	Specifies the model name of the LLDP-MED.
AssetID	Specifies the asset tracking identifier for the LLDP-MED.

Chapter 15: Network Time Protocol

Table 41: Network Time Protocol product support

Feature	Product	Release introduced	Release deprecated
For configuration details, see Administering VOSS.			
NTPv3 client	VSP 4450 Series	VSP 4000 4.0	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 4.2.1	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VSP 8200 4.0	VOSS 8.2
	VSP 8400 Series	VOSS 4.2	VOSS 8.2
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	VOSS 8.2
NTPv3 with SHA authentication	VSP 4450 Series	VOSS 5.1	VOSS 8.2
	VSP 4900 Series	VOSS 8.1	VOSS 8.2
	VSP 7200 Series	VOSS 5.1	VOSS 8.2
	VSP 7400 Series	VOSS 8.0	VOSS 8.2
	VSP 8200 Series	VOSS 5.1	VOSS 8.2
	VSP 8400 Series	VOSS 5.1	VOSS 8.2
	VSP 8600 Series	VSP 8600 4.5	Not applicable
	XA1400 Series	VOSS 8.0.50	VOSS 8.2
NTPv4 client for IPv4	VSP 4450 Series	VOSS 7.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 7.0	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 7.0	Not applicable
	VSP 8400 Series	VOSS 7.0	Not applicable
	VSP 8600 Series	VSP 8600 8.0	Not applicable
	XA1400 Series	Not Supported	Not applicable
NTPv4 client for IPv6	VSP 4450 Series	VOSS 7.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable

Table continues…

Feature	Product	Release introduced	Release deprecated
	VSP 7200 Series	VOSS 7.0	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 7.0	Not applicable
	VSP 8400 Series	VOSS 7.0	Not applicable
	VSP 8600 Series	VSP 8600 8.0	Not applicable
	XA1400 Series	Not Supported	Not applicable
NTPv4 master and restrict	VSP 4450 Series	VOSS 8.0	Not applicable
	VSP 4900 Series	VOSS 8.1	Not applicable
	VSP 7200 Series	VOSS 8.0	Not applicable
	VSP 7400 Series	VOSS 8.0	Not applicable
	VSP 8200 Series	VOSS 8.0	Not applicable
	VSP 8400 Series	VOSS 8.0	Not applicable
	VSP 8600 Series	VSP 8600 8.0 demonstration feature	Not applicable
	XA1400 Series	Not Supported	Not applicable

Note:

DEMO FEATURE - NTPv4 Master Mode and Restrict is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information, see VOSS Feature Support Matrix.

The following sections provide information on NTPv3 and NTPv4. If your platform supports both versions, the default is NTPv3.

Important:

For NTPv4:

- The switch can operate as both NTPv4 client and NTPv4 server.
- The server selection algorithm can deem a server to be unfit to sync even though there is connectivity.
- It can take several iterations (intervals) for the server to sync.
- You need to configure a Segmented Management Instance on applicable switches before you use NTPv4.

NTP fundamentals

This section provides conceptual material about the Network Time Protocol (NTP). Review this content before you make changes to the NTP configuration.

NTP Overview

NTP synchronizes the internal clocks of various network devices across large, diverse networks to universal standard time. NTP protocol runs over the User Datagram Protocol (UDP), which in turn runs over IP.

The NTPv3 specification is documented in RFC 1305 and supports IPv4 addresses.

Note:

NTPv3 is only supported on VSP 8600 Series.

The NTPv4 specification is documented in RFC 5905 and supports both IPv4 and IPv6 addresses.

Every network device relies on an internal system clock to maintain accurate time. On local devices, the internal system clock is typically manually set 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 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.

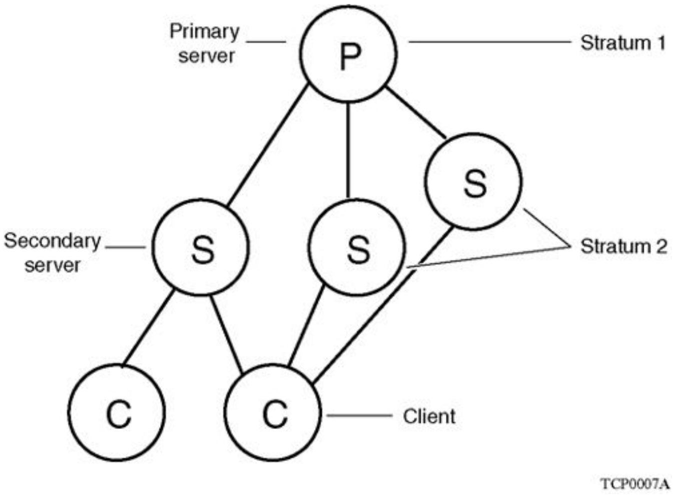


Figure 3: NTP time servers forming a synchronization subnet

In the NTP model, the synchronization subnet 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 NTP system implementation model on page 341. 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. 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. 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.

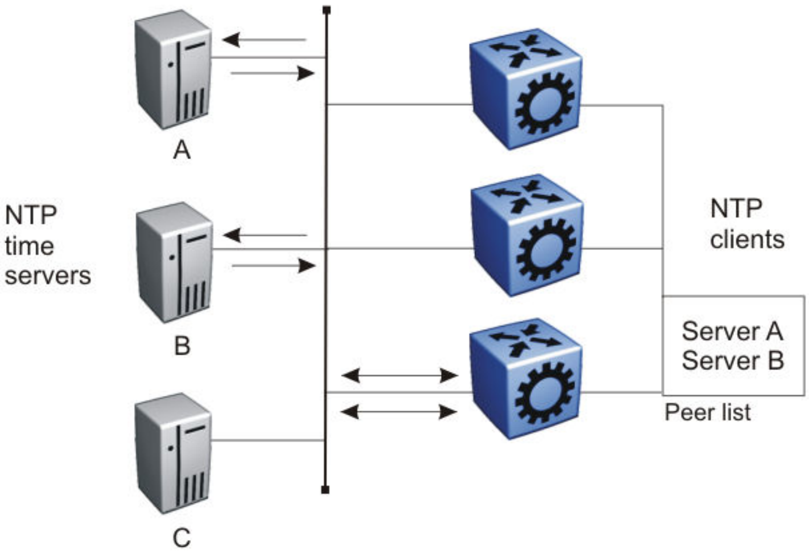


Figure 4: NTP Time Servers Operating in Unicast Client Mode

NTP Master Mode

Note:

DEMO FEATURE - NTPv4 Master Mode is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

The switch can operate as both an NTPv4 client and an NTPv4 server. You can configure the NTPv4 server by enabling the master mode. When the master mode is configured, peers can synchronize themselves with the local clock when the NTPv4 server loses synchronization or if an external NTPv4 source is not reachable. For information about configuring NTPv4 server master mode, see Configuring NTP Master Mode on page 352 and Configure NTP Globally on page 358.

NTP Restrict

Note:

DEMO FEATURE - NTPv4 Restrict is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

The switch offers the restrict capability on the NTPv4 server. When the NTPv4 server master mode is disabled, the restrict capabilities are disabled by default. All IPv4 or IPv6 addresses or networks except for those addresses configured as servers are ignored. For addresses configured as servers, traffic is allowed but there are some default restriction values.

When the NTPv4 server master mode is enabled, there are no restrict rules configured, which means all connections are allowed or there are one or multiple rules configured and only those addresses or networks with the configured rules are allowed. For more information about creating NTP restrict entries, see Creating NTP Restrict Entries on page 353.

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.

Configuring NTP 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:

- NTPv3 does not use the Segmented Management Instance. For NTPv3, configure a traditional IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see Configuring IPv4 Routing for VOSS or Configuring IPv6 Routing for VOSS.

  Note:

  NTPv3 is only supported on VSP 8600 Series.

- For NTPv4, you must create a Segmented Management Instance and configure routing for that instance.

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.

The following task flow diagram shows the sequence of procedures you perform to configure NTP.

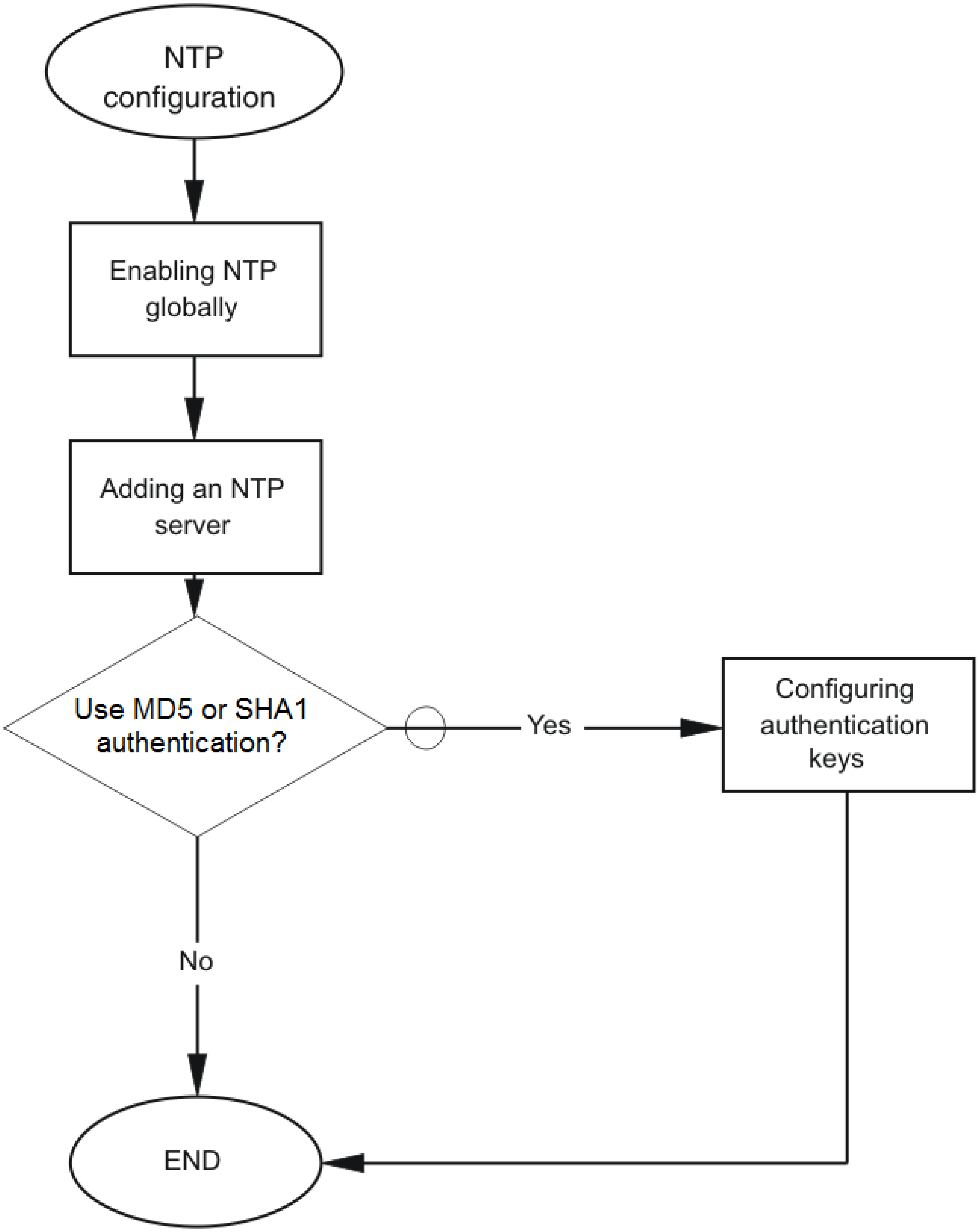


Figure 5: NTP Configuration Procedures

Configure the NTP Version

✱ **Note:**

This procedure only applies to VSP 8600 Series.

Configure the switch to use NTPv3 or NTPv4. The default is NTPv3.

Before you begin

You must globally disable NTP before you change the version.

About this task

NTPv3 supports IPv4 addresses. NTPv4 supports both IPv4 and IPv6 addresses.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the version:

   ```
   ntp version <3 | 4>
   ```

Enable 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)** Configure the NTP interval time (between successive NTP updates):

   ```
   ntp interval <1-2185>
   ```

   OR

   ```
   ntp interval <4-17>
   ```

3. Enable NTP globally:

   ```
   ntp
   ```

4. Confirm the global configuration:

   ```
   show ntp
   ```

Example

Specify the time interval between NTP updates, and then enable NTP globally.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp interval 10
Switch:1(config)#ntp
```

Confirm the configuration:

```
Switch:1(config)#show ntp

=========================================================================================
                                   NTP Master
=========================================================================================
Version   Enabled    Stratum
-----------------------------------------------------------------------------------------
4         False      10

=========================================================================================
                                   NTP Client
=========================================================================================
Version  Enabled   Interval  Last Update Time                Synchronized To
-----------------------------------------------------------------------------------------
3        True      10        Thu Jul 18 08:32:59 2019 EDT    192.0.2.0 (Stratum:2)
```

```
Switch:1(config)#show ntp

==========================================================================================
                                      NTP
==========================================================================================
Version   Enabled        Interval    Last Update Time                  Synchronized To
------------------------------------------------------------------------------------------
3         True           10
```

Variable Definitions

The following table defines parameters for the **ntp** command.

Variable	Value
authentication-key <1–65534> WORD<0–20>	Creates an authentication key for MD5 or SHA1 authentication. To configure this option to the default value, use the default operator with the command. The default configuration is to delete the authentication key. 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.
type *<md5 | sha1>*	Specifies the type of authentication as MD5 or SHA1. The default is MD5 authentication.
interval*<1–2185>* **OR** *<4-17>* **Note:** Exception: interval range 1-2185 is only supported on VSP 8600 Series.	Specifies the interval value in minutes. The default for NTPv3 is 15 minutes. The default for NTPv4 is 6 minutes.

Table continues…

Variable	Value
	To restore the NTP interval to the default value, use the **`default ntp interval`** command. ✱ **Note:** Exception: NTPv3 is only supported on VSP 8600 Series. v

Add an NTP Server

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.

About this task

For NTPv3, you can configure a maximum of 10 IPv4 NTP servers.

✱ **Note:**

NTPv3 is only supported on VSP 8600 Series.

For NTPv4, this procedure adds the NTP server information to the switch that is acting as an NTP client. You can configure a maximum of 10 IPv4 NTP servers and 10 IPv6 NTP servers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Add an NTP server:

   ```
   ntp server WORD<0-255>
   ```

3. Configure additional options for the NTP server:

   ```
   ntp server WORD<0-255> [auth-enable] [authentication-key <0-65534>]
   [enable] [source-ip WORD<0-46>]
   ```

   ✱ **Note:**

   The source-ip parameter applies only to NTPv3 on VSP 8600 Series.

   The NTP server is automatically enabled by default.

4. Confirm the configuration:

   ```
   show ntp server
   ```

Example

```
Switch:>enable
Switch:1configure terminal
Switch:1(config)#ntp server 192.0.2.187
```

The output for the **`show ntp server`** command includes different information for NTPv3 and NTPv4.

For NTPv3:

```
Switch:1(config)#show ntp server

==========================================================================================
                                   NTP Server
==========================================================================================
Server Ip         Enabled Auth    Key Id     Source IP         Auth Type
------------------------------------------------------------------------------------------
192.0.2.187       true    false   0          0.0.0.0           N/A
```

For NTPv4:

```
Switch:1(config)#show ntp server

==========================================================================================
                                   NTP Server
==========================================================================================
Server Ip                                Enabled Auth    Key Id     Auth Type
------------------------------------------------------------------------------------------
192.0.2.187                              true    false   0          N/A
```

Variable Definitions

The following table defines parameters for the **`ntp server`** command.

Variable	Value
auth-enable	Activates MD5 or SHA1 authentication on this NTP server. Without this option, the NTP server will not have any authentication by default.
authentication-key <0-65534>	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.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.
source-ip WORD<0–46> **Note:** Exception: only supported on VSP 8600 Series.	Specifies the source IP for the server. If you do not configure this parameter, by default, the source IP entry is initialized to 0.0.0.0. The IP address specified can be any local interface. The source-ip parameter applies only to NTPv3.
WORD<0–255>	Specifies the IPv4 or IPv6 address of the NTP server.

Configuring Authentication Keys

About this task

Configure up to 10 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 <1-65534> WORD<0-20> [type <md5|sha1>]`

3. Enable MD5 or SHA1 authentication for the server:

   `ntp server WORD<0-255> auth-enable`

4. Assign an authentication key to the server:

   `ntp server WORD<0-46> authentication-key <0-65534>`

   Note:

   If you must disable authentication on the server, you must also disable authentication on the switch for example: `no ntp server WORD<0-255> auth-enable`

5. Confirm the configuration:

   `show ntp key`

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp authentication-key 5 SecretKey type md5
Switch:1(config)#ntp server 192.0.2.187 auth-enable
Switch:1(config)#ntp server 192.0.2.187 authentication-key 5
Switch:1(config)#show ntp key
==========================================================================================
                                    NTP Key
==========================================================================================
Key_Id      Key                             Type
------------------------------------------------------------------------------------------
5           SecretKey                       MD5
10          a                               SHA1
20          abcdef&^%#1112                  MD5
30          1234567abcdtest                 SHA1
100         b                               MD5
```

Variable Definitions

The following table defines parameters for the **`ntp`** and **`ntp server`** commands.

Variable	Value
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 <1-65534> 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 <0-65534>	Specifies the key ID value used to generate the MD5 or SHA1 digest for the NTPv4 server. 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.
WORD<0–255>	Specifies the IPv4 or IPv6 address of the server.

Configuring NTP Master Mode

About this task

Note:

DEMO FEATURE - NTPv4 Master Mode is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Perform the following procedure to set the switch to act as the Network Time Protocol (NTP) server, which means it will run in the master mode. The default value is disabled. You can also enable NTP master mode for a specific stratum.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable NTP master:

   ```
   ntp master
   ```

3. **(Optional)** Configure NTP master for a specific stratum:

   ```
   ntp master <1-16>
   ```

4. Verify the configuration:

   ```
   show ntp
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp master
Switch:1(config)#show ntp
==========================================================================================
                                   NTP Master
==========================================================================================
Version   Enabled        Stratum
------------------------------------------------------------------------------------------
4         True           11

==========================================================================================
                                   NTP Client
==========================================================================================
Version   Enabled        Interval    Last Update Time                   Synchronized To
------------------------------------------------------------------------------------------
3         False          60
```

Variable Definitions

The following table defines parameters for the **`ntp master`** command:

Variable	Value
<1-16>	Specifies a stratum value. The default value is 10. **Note:** If there is a better stratum available, it is preferred than what is configured.

Creating NTP Restrict Entries

Note:

DEMO FEATURE - NTPv4 Restrict is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Perform the following procedure to configure the NTP restrict capability for a specific IPv4 or IPv6 address(es), which means the switch permits NTP traffic flow from the specified IP addresses only. By default the NTP restrict capability is disabled.

Note:

- You can configure a maximum of 128 NTP Restrict entries (IPv4 or IPv6 addresses).
- 0.0.0.0/0 or ::/0 NTP restrict entries are equivalent to no NTP restrict rules configured.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure a specific NTP restrict IP address:

   ```
   ntp restrict WORD<0-255>
   ```

3. Verify the restricted IP address:

   ```
   show ntp restrict
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ntp restrict 192.0.0.0
Switch:1(config)#show ntp restrict
================================================================================
                            NTP Restrict Information
================================================================================
TYPE     ADDRESS                                          MASK/PREFIX LEN
--------------------------------------------------------------------------------
IPv4     192.0.0.0                                          23
--------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for the **`ntp restrict`** command:

Variable	Value
WORD<0-255>	Specifies the IPv4 or IPv6 address. **Note:** You can configure a maximum of 128 IPv4 and IPv6 addresses in the NTP restrict list.

Example of NTPv3 Configuration to NTPv4 Migration

Note:

This procedure only applies to VSP 8600 Series.

Procedure

1. Configure a Segmented Management Instance.

   ```
   Switch:1(config)#mgmt vlan 10
   Switch:1(mgmt:vlan)#ip address 192.0.2.1/24
   Switch:1(mgmt:vlan)# enable
   ```

   OR

   ```
   Switch:1(config)#mgmt clip
   Switch:1(mgmt:clip)#ip address 198.51.100.1/32
   Switch:1(mgmt:clip)#enable
   ```

2. Configure routing for the Management Instance.

   For the VLAN interface, create a static route to reach the NTP server:

   ```
   Switch:1(config)#mgmt vlan
   Switch:1(mgmt:vlan)#ip route 203.0.113.1/24 next-hop 192.0.2.2
   ```

   OR for the CLIP interface:

   ```
   Switch:1(config)#router ospf
   Switch:1(config-ospf)#redistribute direct
   Switch:1(config-ospf)#redistribute direct enable
   Switch:1(config-ospf)#exit
   Switch:1(config)#ip ospf apply redistribute direct
   ```

3. Verify connectivity between the Management Instance and the NTPv4 server.

   ```
   Switch:1(config)#ping 203.0.113.1 mgmt
   ```

4. Disable NTP globally.

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

5. Change the NTP version.

   ```
   Switch:1(config)#ntp version 4
   ```

6. Enable NTP globally.

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

7. Enable NTP master.

   ```
   Switch:1(config)#ntp master
   ```

Configuring NTP 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:

- NTPv3 does not use the Segmented Management Instance. For NTPv3, configure a traditional IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see Configuring IPv4 Routing for VOSS or Configuring IPv6 Routing for VOSS.

  Note:

  NTPv3 is only supported on VSP 8600 Series.

- For NTPv4, you must create a Segmented Management Instance and configure routing for that instance.

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.

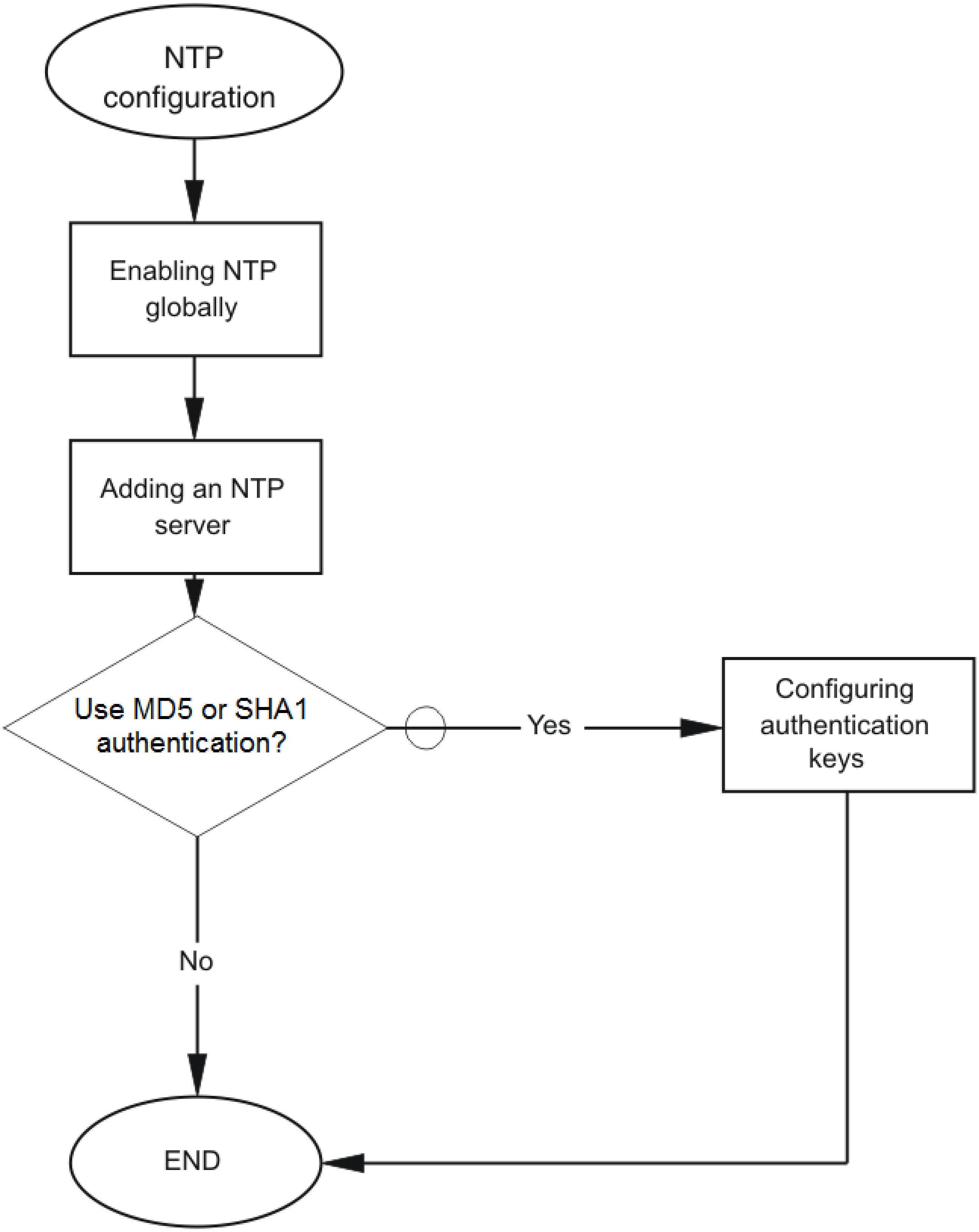


Figure 6: NTP Configuration Procedures

Configure NTP Globally

Note:

DEMO FEATURE - NTPv4 Master Mode is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can use the following procedure to globally enable NTP. For the VSP 8600 Series, you can configure the NTP version.

You can also enable master mode on the NTP server configured on the switch. When the master mode is configured, peers can synchronize themselves with the local clock when the NTP server loses synchronization or if an external NTP source is not reachable.

Before you begin

You must globally disable NTP before you change the version.

About this task

NTPv3 supports IPv4 addresses. NTPv4 supports both IPv4 and IPv6 addresses.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **NTP**.
2. Select **General**.
3. Select the **Globals** tab.
4. Select **Enable**.
5. Enter a time interval.
6. **Note:**

   This step only applies to VSP 8600 Series.

   Select the NTP version.
7. **(Optional)** To configure the switch as an NTP server, in the **NTP Master** section, select **Enable**.
8. In the **Stratum** field, enter a value.
9. Select **Apply**.

Globals Field Descriptions

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

NTP Client section:

Name	Description
Enable	Enables the client NTP server. By default, NTP is disabled.
Interval ✱ **Note:** Exception: NTPv3 is only supported on VSP 8600 Series.	Specifies the time interval (in minutes) between successive NTP updates. The default values are: • NTPv3: 15 minutes • NTPv4: 6 minutes
Version ✱ **Note:** Exception: only supported on VSP 8600 Series.	Configures the NTP version. The default is NTPv3.

NTP Master section:

Name	Description
Enable	Enables master mode for the configured NTP server. The default value is disabled.
Stratum	Specifies the stratum for the master NTP server. The default value is 10. ✱ **Note:** If a better stratum is available, it is preferred over what is configured.

Add an NTPv3 Server

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.

✱ **Note:**

This procedure is only supported on VSP 8600 Series.

About this task

For NTPv3, you can configure a maximum of 10 IPv4 NTP servers.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **NTP**.
2. Select **NTPv3**.
3. Select the **Server** tab.
4. Select **Insert**.

5. Specify the IP address of the NTP server.
6. Select **Insert**.

Server Field Descriptions

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

Name	Description
ServerAddressType	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. The default is 0, which indicates that authentication is disabled.
AccessAttempts	Specifies the number of NTP requests sent to this NTP server.
Success	Specifies the number of times this NTP server updated the time.
Failure	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 reachability of the server.
Synchronized	This variable is the status of synchronization with the server.
SourceIpAddr **Note:** Exception: only supported on VSP 8600 Series.	Specifies the source IP for the server. If you do not configure a source IP, by default, the entry is initialized to 0.0.0.0. The IP address specified can be any local interface.

Configure Authentication Keys for NTPv3

Assign an NTP key to use MD5 or SHA1 authentication on the server.

Note:

This procedure is only supported on VSP 8600 Series.

Procedure

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

2. Select **NTPv3**.
3. Select the **Key** tab.
4. Select **Insert**.
5. Specify the secret key.
6. Select **Insert**.

Key field descriptions

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

Name	Description
KeyId	Specifies the key ID that generates the MD5 or SHA1 digest.
KeySecret	Specifies the MD5 or SHA1 key that generates the MD5 or SHA1 digest. You must specify an alphanumeric string.
KeyType	Specifies the type of authentication, whether MD5 or SHA1. The default is MD5 authentication.

Add an NTPv4 Server

Add a remote NTP server to the configuration by first 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.

About this task

For NTPv4, this procedure adds the NTP server information to the switch that is acting as an NTP client. You can configure a maximum of 10 IPv4 NTP servers and 10 IPv6 NTP servers.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **NTP**.
2. Click **NTPv4**.
3. Click the **Server** tab.
4. Click **Insert**.
5. Specify if the IP address is IPv4 or IPv6.
6. Specify the IP address of the NTP server.
7. Click **Insert**.

Server field descriptions

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

Name	Description
ServerAddressType	Specifies the address type as IPv4 or IPv6.
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. The default is 0, which indicates that authentication is disabled.
Stratum	Shows the stratum of the server.
Version	Shows the NTP version of the server.
Broadcast	Shows if broadcast is enabled or disabled
AuthEnabled	Shows if authentication is enabled or disabled
AuthStatus	Shows the authentication status.
Synchronized	Shows the status of synchronization with the server.
Reachable	Shows the NTP reachability status of the server.
RootDelay	Shows the root delay of the server.
RootDisp	Shows the root dispersion of the server.
ServerDelay	Shows the delay of the server.
Dispersion	Shows the dispersion of the server.
Offset	Shows the offset of the server.
Precision	Shows the NTP precision of the server in seconds.
Jitter	Shows the jitter of the server
LastEvent	Shows the last event of the server.

Configure Authentication Keys for NTPv4

Assign an NTP key to use MD5 or SHA1 authentication on the server.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **NTP**.
2. Click **NTPv4**.
3. Click the **Key** tab.
4. Click **Insert**.
5. Complete the fields.
6. Click **Insert**.

Key field descriptions

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

Name	Description
KeyId	Specifies the key ID that generates the MD5 or SHA1 digest.
KeySecret	Specifies the MD5 or SHA1 key that generates the MD5 or SHA1 digest. You must specify an alphanumeric string.
KeyType	Specifies the type of authentication as MD5 or SHA1. The default is MD5 authentication.

Creating NTPv4 Restrict Entries

Note:

DEMO FEATURE - NTPv4 Restrict is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Perform the following procedure to configure the NTP restrict capability for a specific IPv4 or IPv6 address(es), which means the switch permits traffic flow from the specified IP address only. By default the NTP restrict capability is disabled.

Note:

- You can configure a maximum of 128 NTP Restrict entries (IPv4 or IPv6 addresses).
- 0.0.0.0/0 or ::/0 NTP restrict entries are equivalent to no NTP restrict rules configured.

Before you begin

You must enable NTPv4 server master mode. For more information, see Configure NTP Globally on page 358.

Procedure

1. In the Navigation pane, expand **Configuration** > **Edit** > **NTP**.
2. Click **Restrict**.
3. Click the **Restrict Info** tab.
4. Click **Insert**.
5. In the **RowIndex** field, enter a value.
6. Select the IP address type.
7. Enter the IPv4 or IPv6 address.
8. Enter the restrict mask value.
9. Click **Insert**.

Restrict Info Field Descriptions

Use data in the following table to use the Restrict Info tab.

Name	Description
RowIndex	Specifies the NTP Restrict entry.
AddressType	Specifies the NTP Restrict address type.
RestrictAddress	Specifies the NTP address to be restricted.
RestrictMask	Specifies the prefix length of the IPv4 or IPv6 NTP address to be restricted.

Chapter 16: Secure Shell

Table 42: Secure Shell product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Secure Shell (SSH) server (IPv4)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
Secure Shell (SSH) client (IPv4)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
Secure Sockets Layer (SSL) certificate management	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported
SSH server (IPv6)	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1

Table continues…

Feature	Product	Release introduced
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	Not Supported
SSH client (IPv6)	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0
	XA1400 Series	Not Supported
SSH client disable	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
SSH key sizes in multiples of 1024 **Note:** VOSS Releases 6.0 and 6.0.1 do not support this change.	VSP 4450 Series	VOSS 5.1.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1.2
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1.2
	VSP 8400 Series	VOSS 5.1.2
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	Not Supported
SSH rekey	VSP 4450 Series	VOSS 5.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 5.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	VOSS 5.1
	VSP 8600 Series	VSP 8600 6.1
	XA1400 Series	VOSS 8.1

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 390.

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).

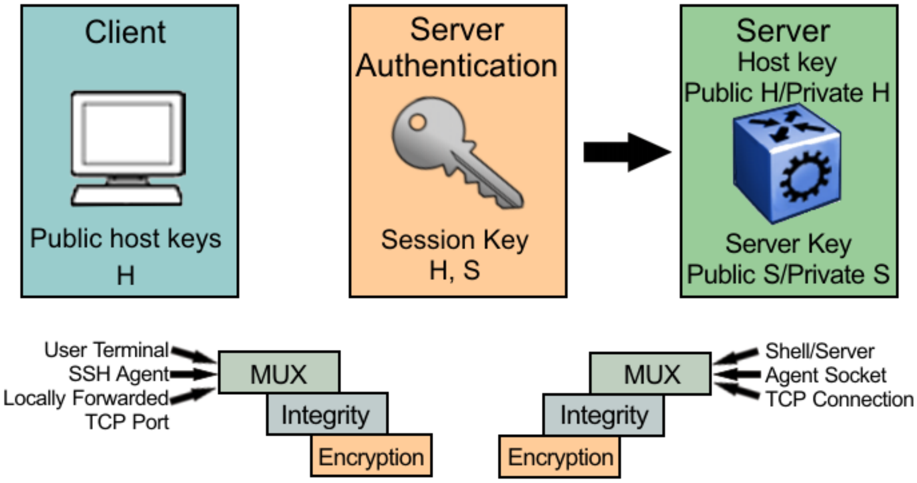


Figure 7: Overview of the SSHv2 protocol

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 Third-party SSH and SCP client software on page 375. The switch also supports outbound connections to remote SSHv2 servers to provide complete inbound and outbound secure access.

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 .DSA authentication access level and file name on page 376.

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.

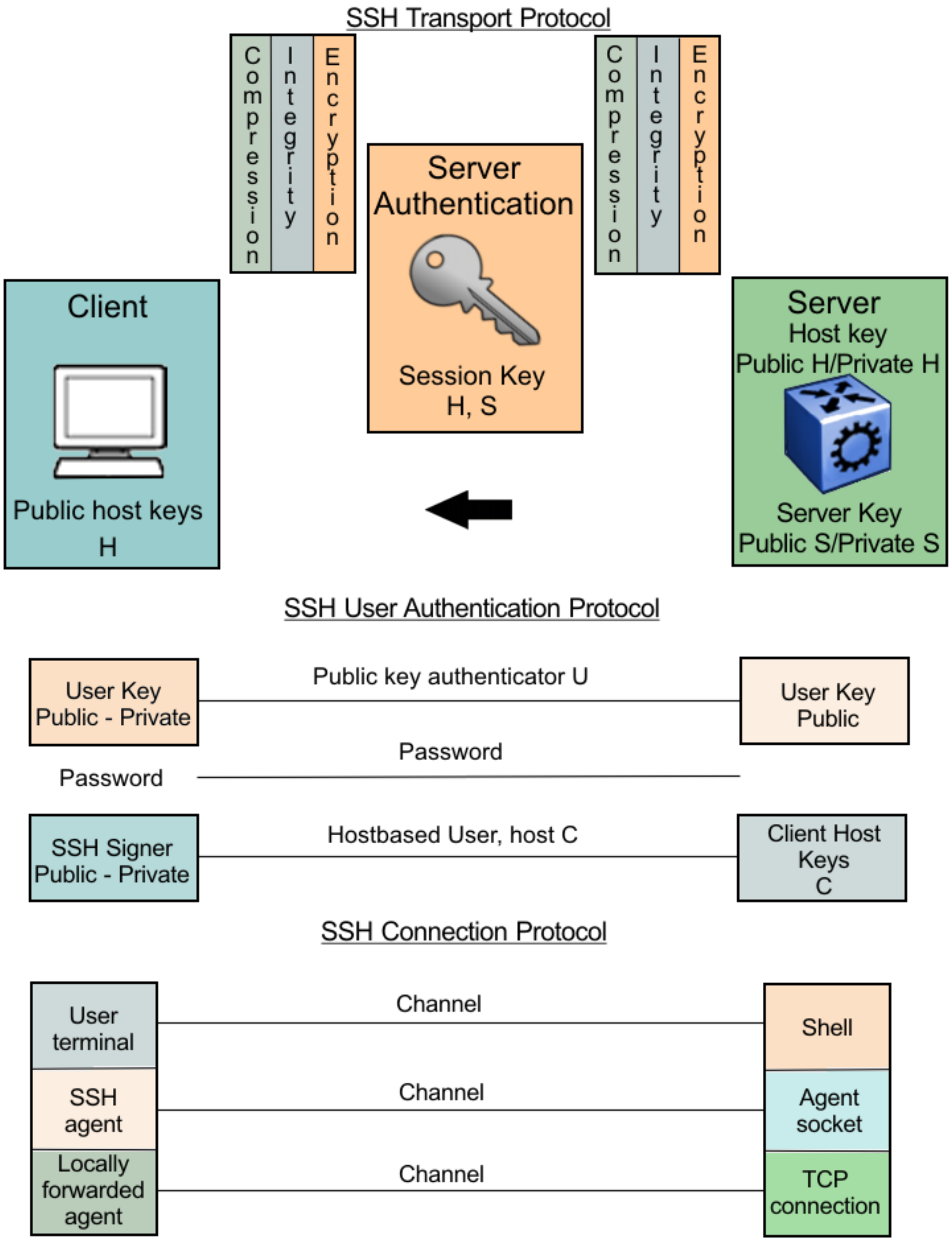


Figure 8: Separate SSH version 2 protocols

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.

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.

Note:

SCP is supported for RWA users only. RW or R level will not work and the switch logs a message on the device.

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 we recommend 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, remote login (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.

Note:

rlogin is supported only on the VSP 8600 Series.

You can disable block-snmp after you enable SSHv2 secure mode, and you can connect again using COM.

User ID Logs

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 43: 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)	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
	• auditor —/intflash/.ssh/id_dsa_auditor (private key), /intflash/.ssh/id_dsa_auditor.pub (public key) • 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

Tested 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 44: 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:	• Client distribution includes an SCP client that is supported on switch.

Table continues…

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
	- 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.	
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 DSA authentication access level and file name on page 376 for proper naming convention.

If a DSA key pair does not exist, you can generate the DSA key pair using the **`ssh dsa-user-key [WORD<1-15>] [size <1024-1024>]`** 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 DSA authentication access level and file name on page 376.

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 45: 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 46: 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

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.

Configure Secure Shell using CLI

Use Secure Shell version 2 (SSHv2) to enable secure communications support over a network for authentication, encryption, and network Integrity.

Before you begin

- Disable the sshd daemon. All SSHv2 commands, except enable, require that you disable the sshd daemon.
- Set the user access level to read/write/all community strings.
- Disable all nonsecure access services. It is recommended that you disable the following services: Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Telnet, and Remote login (rlogin). For more information about disabling access services, see Enable Remote Access Service on page 90.

  Note:

  Rlogin is only supported on VSP 8600 Series.
- Use the console port to configure the SSHv2 parameters. Depending on your hardware platform, the console port displays as console or 10101.

Enabling the SSHv2 server

Enable the SSHv2 server to provide secure communications for accessing the switch. The switch does not support SSHv1.

Before you begin

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

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable keyboard-interactive authentication:

   ```
   ssh keyboard-interactive-auth
   ```

Configure SSH Configuration Parameters

Note:

DEMO FEATURE - Two-Factor Authentication–X.509v3 Certificates for SSH is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

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. Configure the authentication type to use:

   ```
   ssh authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]}
   ```

3. Enable DSA authentication:

   ```
   ssh dsa-auth
   ```

4. Generate a new DSA host key:

   ```
   ssh dsa-host-key [<1024-1024>]
   ```

5. Generate a new SSH DSA user key:

   ```
   ssh dsa-user-key WORD<1-15> [size [<1024-1024>]]
   ```

6. Configure the type of encryption to use:

   ```
   ssh encryption-type {[3des-cbc][aead-aes-128-gcm-ssh ][aead-aes-256-gcm-ssh] [aes128-cbc][aes128-ctr][aes192-cbc][aes192-ctr][aes256-cbc][aes256-ctr][blowfish-cbc] [rijndael128-cbc][rijndael192-cbc]}
   ```

7. Configure the key-exchange to use:

   ```
   ssh key-exchange-method {[diffie-hellman-group1-sha1][diffie-hellman-group14-sha1]}
   ```

8. Configure the maximum number of SSH sessions:

   ```
   ssh max-sessions <0-8>
   ```

9. Enable password authentication:

    `ssh pass-auth`

10. Configure the SSH connection port:

    `ssh port <22,1024..49151>`

11. Enable RSA authentication:

    `ssh rsa-auth`

12. Generate a new RSA host key:

    `ssh rsa-host-key [<1024–2048>]`

13. Generate a new RSA user key.

    `ssh rsa-user-key WORD<1–15>`

14. Enable X.509 V3 authentication:

    `ssh x509v3-auth enable`

15. Configure X.509 V3 revocation:

    `ssh x509v3-auth revocation-check-method {none | ocsp}`

16. Configure X.509 V3 username:

    `ssh x509v3-auth username {overwrite | strip-domain | use-domain WORD<1-254>}`

17. Enable SSH secure mode:

    `ssh secure`

18. Configure the authentication timeout:

    `ssh timeout <1-120>`

19. Configure the SSH version:

    `ssh version <v2only>`

20. 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

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

Variable	Value
authentication-type *{[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256]}*	Specifies the authentication type. Select from one of the following: • aead-aes-128-gcm-ssh • aead-aes-256-gcm-ssh • hmac-sha1 • hmac-sha2-256 Use the no operator before this parameter, no ssh authentication-type {[aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [hmac-sha1] [hmac-sha2-256] }, to disable the authentication type. To disable all authentication types use the command no ssh authentication-type.
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 *<1024–1024>*	Generates a new SSH DSA host key. The DSA host key size 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.

Table continues…

Variable	Value
	• 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, 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.
encryption-type *{[3des-cbc] [aead-aes-128-gcm-ssh] [aead-aes-256-gcm-ssh] [aes128-cbc][aes128-ctr] [aes192-cbc][aes192-ctr] [aes256-cbc][aes256-ctr] [blowfish-cbc] [rijndael128-cbc] [rijndael192-cbc]}*	Configures the encryption-type. Select an encryption-type from one of the following: • 3des-cbc • aead-aes-128-gcm-ssh • aead-aes-256-gcm-ssh • aes128-cbc • aes128-ctr • aes192-cbc • aes192-ctr • aes256-cbc • aes256-ctr • blowfish-cbc • rijndael128-cbc • rijndael192-cbc Use the no operator before this parameter `no ssh encryption-type {[3des-cbc][aead-aes-128-gcm-ssh ][aead-aes-256-gcm-ssh] [aes128-cbc][aes128-ctr][aes192-cbc][aes192-ctr] [aes256-cbc][aes256-ctr][blowfish-cbc] [rijndael128-cbc][rijndael192-cbc]}` to disable the encryption type. To disable all authentication types use the command `no ssh encryption-type`.
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.

Table continues…

Variable	Value
port *<22,1024–49151>*	Configures the Secure Shell (SSH) connection port. *<22,1024 to 49151>* is the TCP port number. The default is 22. **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 *WORD<1–15>*	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.
rsa-user-key *[<1024–2048>]*	Generates a new SSH RSA 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 value 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

Table continues…

Variable	Value
	• 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 rsa-user-key WORD<1-15>`, to disable SSH RSA user key.
secure **Note:** Exception: rlogin only supported on VSP 8600 Series.	Enables SSH in secure mode and immediately disables the access services SNMP, FTP, TFTP, remote login (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.
x509v3-auth *enable*	Configures X.509 V3 authentication. The default is enabled. Use the no operator before the parameter, `no ssh x509v3-auth enable`, to disable X.509 V3 authentication. Use the no operator before the parameter, `no ssh x509v3-auth username`, to disable X.509 V3 username. **`x509v3-auth`** is available for demonstration purposes on some products. For more information, see VOSS Feature Support Matrix.
x509v3-auth *[revocation-check-method <none|oscp>]*	Configures X.509 V3 authentication revocation check method. The default is OCSP. • none - Specifies no revocation check method. oscp - Specifies Online Certificate Status Protocol (OSCP) as revocation check method. **`x509v3-auth`** is available for demonstration purposes on some products. For more information, see VOSS Feature Support Matrix.
x509v3-auth *[username <overwrite|strip-domain|use-domain WORD<1-254>]*	Configures X.509 V3 username configuration. The default is disabled. • overwrite - Specifies the switch to send the principal name and domain name from the certificate to the RADIUS server for authorization. strip-domain - Specifies the switch to send the princial name from the certificate without the domain name to the RADIUS server for authorization.

Table continues…

Variable	Value
	use-domain `WORD<1-254>` - Specifies the switch to send the principal name from the certificate, with the domain name you entered to the RADIUS server for authorization. Use the no operator before the parameter, `no ssh x509v3-auth username`, to disable X.509 V3 username. **`x509v3-auth`** is available for demonstration purposes on some products. For more information, see VOSS Feature Support Matrix.

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. To enter User EXEC mode, log on to the switch.
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                  : false
        dsa-auth                  : true
        pass-auth                 : true
        keyboard-interactive-auth : false
        sftp enable               : true
        enable                    : true
        authentication-type       : aead-aes-128-gcm-ssh aead-aes-256-gcm-ssh hmac-sha1
hmac-sha2-256
        encryption-type           : 3des-cbc aead-aes-128-gcm-ssh aead-aes-256-gcm-ssh
aes128-cbc aes128-ctr
                                    aes192-cbc aes192-ctr aes256-cbc aes256-ctr blowfish-
cbc rijndael128-cbc
                                    rijndael192-cbc
        key-exchange-method       : diffie-hellman-group1-sha1 diffie-hellman-group14-sha1
```

Variable Definitions

The following table defines parameters for the**`show ssh`** command.

Variable	Value
global	Display global system SSH information.
session	Display the current session SSH information.

Connect 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

The following table defines parameters for 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 <1024-1024>]
   ```

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:
   1. Create the DSA user key file:

      ```
      ssh-keygen -t dsa
      ```

   2. 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 1024 bits:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ssh dsa-user-key rwa size 1024
```

Variable Definitions

The following table defines parameters for 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.

Table continues…

Variable	Value
	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, 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 *<1024–1024>*	Specifies the size of the DSA user key. The default is 1024 bits.

Managing an SSL certificate

The TLS server selects the server certificate in the following order:

1. A certification authority (CA)-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.
2. A self-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.

If the server certificates are not available, the TLS server generates a new self-signed certificate at startup and uses that by default. The self-signed certificate is available in `/.intflash/.cert/.ssl`. You can choose to use an online or offline CA-signed certificate, which will take precedence over the self-signed certificate.

For more information about SSL certificate manipulation, see Configuring Security for VOSS.

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

The following table defines parameters for 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 532.

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

The following table defines parameters for 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

The following table defines parameters for 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

The following table defines parameters for 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
```

Downgrading or Upgrading from Releases that Support Different Key Sizes

Use this procedure if you need to downgrade or upgrade from a release that supports different key sizes.

Different releases can support different DSA host key, RSA host key, and DSA user key sizes. If you need to upgrade or downgrade to an earlier release that does not support the same key size, you must delete all of the keys from the .ssh directory and generate new keys for SSH. If you do not do this, key sizes that are no longer supported will no longer function.

You only need to perform this procedure if you have previously generated DSA host, RSA host, or DSA user keys with a release that supports different key sizes.

Procedure

1. Use the following command to disable SSH:

   ```
   no ssh
   ```

2. From the config terminal go to the .ssh directory using the command:

   ```
   cd /intflash/.ssh
   ```

3. After you upgrade or downgrade, delete the following keys from the .ssh directory.

   ```
   ssh_dss.key
   ssh_rsa.key
   moc_sshc_dsa_file
   moc_sshc_rsa_file
   id_dsa_rwa
   id_dsa_rwa.pub
   id_rsa_rwa
   id_rsa_rwa.pub
   moc_sshc_dsa_file_fed
   moc_sshc_rsa_file_fed
   known_hosts
   ssh_ecdsa.key
   dsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
   example: dsa_key_rwa
   rsa_key_<access level like rwa/rw/ro/admin/security/privilege/operator/auditor>,
   example: rsa_key_rwa
   ```

4. Generate a new DSA host key:

   ```
   ssh dsa-host-key [<1024-1024>]
   ```

5. Generate a new SSH DSA user key:

   ```
   ssh dsa-user-key WORD<1-15> [size <1024-1024>]
   ```

6. Generate a new RSA host key:

   ```
   ssh rsa-host-key [<1024-2048>]
   ```

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 Change Secure Shell Parameters on page 396.

Change 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 **Configuration** > **Security** > **Control Path**.
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. In the **AuthType** section, select the authentication types you want.

16. In the **Encryption Type** section, select the authentication types you want.
17. In the **KeyExchangeMethod** section, select the authentication types you want.
18. Click **Apply**.

SSH Field Descriptions

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

Name	Description
Enable **Note:** Exception: rlogin is only supported on VSP 8600 Series.	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

Table continues…

Name	Description
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.
RekeyEnable ✱ **Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	Enables SSH rekey globally. The default is disabled.
RekeyTimeInterval ✱ **Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, and VSP 8400 Series.	Configures a time interval, after which the key exchange takes place. The default is 1 hour.
RekeyDataLimit ✱ **Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP	Configures the limit for data transmission during the session. The default is 1 GB.

Table continues…

Name	Description
7400 Series, VSP 8200 Series, and VSP 8400 Series.	
SftpEnable	Enables or disables SFTP. You can use this check box to disable SFTP without affecting the SSH status. The default is enabled.
KeyboardInteractiveAuth	Changes the SSH server authentication mode from the default of password authentication to keyboard interactive.
ClientEnable	Enables SSH client functionality on the switch. By default, the SSH client functionality is enabled. To enable the SSH client functionality, SSH must be enabled globally.
AuthType	Specifies the authentication type. Select from one of the following: • hmacSha1 • hmacSha2256 • aeadAes128GcmSsh • aeadAes256GcmSsh By default, all autentication types are selected.
EncryptionType	Configures the encryption-type. Select an encryption-type from one of the following: • aes128Cbc • aes256Cbc • threeDesCbc • aeadAes128GcmSsh • aeadAes256GcmSsh • aes128Ctr • rijndael128Cbc • aes256Ctr • aes192Ctr • aes192Cbc • rijndael192Cbc • blowfishCbc
KeyExchangeMethod	Configures the key-exchange type. Select from one of the following: • diffieHellmanGroup14Sha1 • diffieHellmanGroup1Sha1

Chapter 17: Segmented Management

With Segmented Management, the Management plane (management protocols) is separated from the Control Plane (routing plane) from a process and data-path perpective. Segmented Management is the only method to management switches. One or a combination of the following management interface/management instance types can be used:

- Out-of-Band (OOB) management IP address (IPv4 and/or IPv6)
- In-band Loopback/circuitless IP (CLIP) management IP address (IPv4 and/or IPv6)
- In-band management VLAN IP address (IPv4 and/or IPv6)

Segmented Management provides better security because you cannot reach the management instance from outside the VRF (in case of CLIP) or outside VLAN/I-SID (in case of management VLAN) and because it has a built-in firewall for the management plane. There is also more predictability with symmetric traffic flows for management traffic originating from and terminating on the switch, for instance:

- Sessions originated from switch (client mode) - Source IP of packets is determined based on Management IP stack routing table weights (configurable).
- Sessions connecting to switch (server mode) - Source IP is derived from session connection and reply will go out on management interface packet.

Segmented Management Instance

Table 47: Segmented Management Instance product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Segmented Management Instance - Management Interface CLIP	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0

Table continues…

Feature	Product	Release introduced
	VSP 8600 Series	VSP 8600 8.0
	XA1400 Series	VOSS 8.1.1 - IPv4 only **Note:** VOSS 8.1.50 does not support this feature.
Segmented Management Instance - Management Interface OOB	VSP 4450 Series	VOSS 8.2
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
Segmented Management Instance - Management Interface VLAN	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.1.1 - IPv4 only **Note:** VOSS 8.1.50 does not support this feature.
Segmented Management Instance — ability to migrate VLAN or loopback IP address	VSP 4450 Series	VOSS 8.2
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	VOSS 8.2
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.2
Segmented Management Instance — DHCP Client for Management Interface OOB or Management Interface VLAN	VSP 4450 Series	VOSS 8.2
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	VOSS 8.2

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.2 OOB not supported

This section details administrative tasks to configure a Segmented Management Instance. A Management Instance is required to provide access to specific management applications.

Segmented Management Instance Overview

The Segmented Management Instance provides support for management interfaces that transmit and receive packets directly to and from the system native Linux IP stack. The management interfaces do not route packets through the VOSS networking IP stack.

Management Applications

The following management applications use the Segmented Management Instance directly to transmit or receive packets with segmented management interfaces and addresses.

Note:

The VSP 8600 Series only supports Ping, Traceroute, and NTPv4.

Segmented Management Instance Applications and Protocols	Client	Server	IPv4	IPv6
Digital Certificates	Yes		Yes	
DHCP Client	Yes		Yes	
DNS	Yes		Yes	Yes
FTP	Yes	Yes	Yes	Yes
HTTP/HTTPS		Yes	Yes	Yes
IQAgent	Yes		Yes	
NTPv4	Yes	Yes	Yes	Yes
OVSDB protocol support for VXLAN Gateway	Yes	Yes	Yes	
Ping	Yes	Yes	Yes	Yes
RADIUS	Yes		Yes	Yes
RADIUS Security (RADSec)	Yes		Yes	Yes

Table continues…

Segmented Management Instance Applications and Protocols	Client	Server	IPv4	IPv6
Representational State Transfer Configuration Protocol (RESTCONF)		Yes	Yes	
SSH/SCP/SFTP	Yes (SSH only)	Yes	Yes	Yes
Syslog	Yes		Yes	Yes
TACACS+	Yes		Yes	
Telnet	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes	Yes

The following management applications do not use the Segmented Management Instance directly to transmit or receive packets, but can integrate with segmented management interfaces and addresses.

Segmented Management Instance Applications and Protocols	IPv4	IPv6
Link Layer Discovery Protocol (LLDP)	Yes	Yes
SynOptics Network Management Protocol (SONMP)	Yes	
Sampled Flow (sFlow)	Yes	
Remote Network Monitoring version 2 (RMON2)	Yes	

Note:

The following management applications do not use the Segmented Management Instance and are deprecated in VOSS.

- NTPv3
- Remote Login (rlogin)
- Remote Shell (RSH)

Segmented Management Instance Migration

Before you upgrade to this VOSS release, you must consider your management interface configuration and migration scenario requirements. The Segmented Management Instance requires migration of legacy management interfaces. Backup and save your configuration files off the switch before upgrading to this release.

Note:

Management interface access to the switch can be lost if you do not perform the applicable migration scenarios before upgrading to this release. Loss of management access after an upgrade can result in an automatic roll-back to the previous software version.

You must perform a manual software commit after upgrading from VOSS Release 8.1.5.0 or earlier to this release. Management interface access is required to input the `software commit` CLI command within 10 minutes after the upgrade. If the time expires the system initiates an automatic roll-back to the previous release.

You must ensure your switch is running one of the following VOSS releases before upgrading to this release:

Note:

If your network environment must migrate static IPv6 routes, your switches must be running VOSS Release 8.1.2.0 or later before upgrading to this release.

- VOSS 8.1.0.0 or later for switches running VOSS 8.1.x releases.
- VOSS 8.0.1.0 or later for switches running VOSS 8.0.x releases.
- VOSS 7.1.3.0 or later for switches running VOSS 7.1.x releases.

You must consider the following legacy management interface migration scenarios before upgrading to this release:

Table 48: Management Interface Migration Scenarios

Mgmt Interface	Mgmt Scenario	Migration Description
DVR leaf	Automatic migration during upgrade.	DVR leaf settings migrate automatically during the software upgrade process.
OOB	Automatic migration during upgrade.	Out-of-Band management settings migrate automatically during the software upgrade process.
CLIP	Specify a Circuitless IP (CLIP) interface for migration to management interface before upgrading.	Use the **`migrate-to-mgmt`** command in the Loopback interface configuration CLI to specify the CLIP interface for management before starting the software upgrade process. The loopback IP to migrate can include the configured ISIS IP shortcuts. Save the configuration before upgrading. A Fabric or legacy Layer 3 network typically uses the CLIP management interface.
VLAN	Specify a VLAN interface for migration to management interface before upgrading.	Use the **`migrate-to-mgmt`** command in the VLAN interface

Table continues…

Mgmt Interface	Mgmt Scenario	Migration Description
		configuration CLI mode to specify the VLAN interface for management before starting the software upgrade process. Save the configuration before upgrading. A Layer 2 network typically uses the VLAN management interface, or for restricting management access to a specific subnet or I-SID.

Automatic Migration

Out-of-Band management interface and DVR leaf configurations automatically migrate during the upgrade process. The management port interface, and all associated applications are moved to the Segmented Management Instance in this release.

A DVR leaf has a single management interface that also automatically migrates during the upgrade process to the Segmented Management Instance.

Static Route Migration

When a VLAN designated as management interface or an Out-of-Band management interface migrates to the Segmented Management Instance, static routes might be required for IP reachability. Static routes are always required for Out-of-Band management interfaces but can also be used with in-band VLAN management.

Static route migration is completed by the upgrade process and no commands are necessary to prepare for the migration. The following logic is applied during the upgrade process to the static routes:

- Out-of-Band management interfaces
  - All IPv4 routes in the VRF 512 / mgmtrouter context are moved to the Segmented Management Instance.
  - All IPv6 routes in GRT with a nexthop IP address that exists in the same subnet as the IPv6 address are moved to the Segmented Management Instance.
- In-Band VLAN management
  - All IPv4 routes from the VRF bound to the migrated VLAN and that have a nexthop IP address in the same subnet as the IPv4 address being migrated are moved to the Segmented Management Instance.
  - All IPv6 routes from the VRF bound to the migrated VLAN and that have a nexthop IP address in the same subnet as the IPv6 address being migrated are moved to the Segmented Management Instance.

Consider the following example of In-Band VLAN management. The static route configuration listed below is in the GRT:

```
ip route 192.168.20.0 255.255.255.0 192.168.10.2 weight 1
ip route 192.168.30.0 255.255.0.0 192.168.10.50 weight 1
ip route 192.168.40.0 255.255.255.0 192.168.20.99 weight 1
ip route 192.168.50.0 255.255.255.0 192.168.10.2 weight 1
no ip route 192.168.50.0 255.255.255.0 192.168.10.2 enable
```

The GRT is associated with VLAN 10 with an IP address of 192.168.10.1. This is the VLAN to be migrated. After the upgrade, the 192.168.20.0, 192.168.30.0, and, 192.168.50.0 routes are migrated to the management instance because their nexthop IP address is associated with the 192.168.10.0/24 subnet.

Note:

All routes with a nexthop IP address associated with the subnet are migrated. This includes administratively disabled routes. Administratively disabled routes must be manually deleted after the upgrade if the route is not needed.

Note:

ECMP static route migration is not supported for the Segmented Management Instance. For an ECMP static route, only the first path in the configuration file migrates.

Note:

After upgrading to VOSS Release 8.1.60 or later, any administratively disabled static routes that migrated to the OOB or VLAN Segmented Management Instance subnet become active. Administratively disabled routes must be manually deleted after the upgrade if the route is not needed.

The static route configuration in the Management VLAN configuration block will be the following after the upgrade:

```
mgmt vlan 10
ip address 192.168.10.1/24
ip route 192.168.20.0/24 next-hop 192.168.10.2
ip route 192.168.30.0/16 next-hop 192.168.10.50
ip route 192.168.50.0/24 next-hop 192.168.10.2
```

Segmented Management Instance Migration

In this release you can use the **migrate-to-mgmt** command to move a management VLAN to a different VLAN ID, or a management CLIP to a different VRF. After you complete the command and save the configuration, the migration to management of the selected interface occurs during the next switch reboot. The following is an outline of the steps required for management migration:

- Configure a new or existing VLAN or CLIP management interface using Interface Configuration mode in the CLI (**interface vlan <vlan_id>** or **interface loopback <clip_id>**) or EDM.
- Add required routes to reach management services and subnets from the new interface.
- Test connectivity to the new interface using ping and traceroute, and from the switch to management stations and servers.
- Use the **migrate-to-mgmt** command from the new interface CLI mode.
- Save the configuration and reboot.

  Note:
  During boot, the migrate-to-mgmt settings are parsed and override the existing management interface with the new interface.
- Access and manage the switch from the new interface.

XA1400 Series Management Migration with a Fabric Extend Source IP VLAN

Before VOSS Release 8.1.60 a single IP address could be used for both routing or management, however Segmented Management Instance now separates the routing and management networking stacks. Since `migrate-to-mgmt` can only move an IP from the routing stack to the management stack, see the following scenario for a before and after upgrade process required to manage a XA1400 Series with the Fabric Extend (FE) tunnel Source IP using Segmented Management Instance:

Before upgrading to VOSS Release 8.1.60 or later:

- Configure a CLIP Management Instance or designate an existing loopback IP for migration.
- Save configuration and reboot.

After upgrading to VOSS Release 8.1.60 or later:

- Manage the XA1400 Series using the CLIP Management Instance.
- Create the VLAN Management Instance with the same VLAN ID and IP address as the FE tunnel source VLAN.
- Modify the default route or create static routes to the VLAN Management Instance.
- Manage the XA1400 Series with the VLAN or CLIP Management Instance.

DHCP Client

To support Zero Touch Deployment, a DHCP Client is used for the Segmented Management Instance VLAN management interface or Out-of-Band (OOB) management interface. The DHCP Client configuration supports a VLAN mode, OOB mode, and a cycle mode. DHCP Client cycle mode alternates IP address requests between the VLAN management interface and OOB management interface until an IP address is obtained on one of the interfaces.

You can also manually configure the DHCP Client to request an IPv4 address from a DHCP server for the In-band VLAN management interface, or the OOB management interface, or to cycle requests until an IP address is obtained on a VLAN or OOB management interface. The DHCP Client supports IPv4 addresses only, and cannot be enabled on multiple management interfaces simultaneously.

DHCP Option 43

DHCP option 43 requests specific vendor options from the DHCP server. Only sub-option 226 (EXTREME.cloudiq-ip) is supported to change the value of the ExtremeCloud IQ server IP address on the switch.

With the support of DHCP option 43, DHCP can dynamically configure the IP address of a private/non-public ExtremeCloud IQ server for zero touch deployments when the default ExtremeCloud IQ server (hac.extremecloudiq.com) is not desired.

For information about configuring the switch to support ExtremeCloud IQ, see Configuring User Interfaces and Operating Systems for VOSS.

DHCP Option 43 Configuration Examples

This section provides examples to configure DHCP Option 43 on a Linux server and on Windows Server.

Example

ISC DHCP Server configuration on Linux:

```
/etc/dhcp/dhcpd.conf
default-lease-time 60;
max-lease-time 7200;
option space EXTREME;
option EXTREME.cloudiq-ip code 226 = ip-address;

class "Edge-without-POE" {
      match if (option vendor-class-identifier = "EXTREME");
      vendor-option-space EXTREME;
      option EXTREME.cloudiq-ip 10.16.231.131;
}

subnet 30.30.30.0 netmask 255.255.255.0 {
        pool {
                range 30.30.30.10 30.30.30.20;
                allow members of "Edge-without-POE";
        }
        option domain-name-servers 10.1.10.1;
        option domain-name "labs.extremenetworks.com";
        option routers 30.30.30.250;
        default-lease-time 3600;
}
```

Example

Windows Server configuration:

1. Go to scope options for defined DHCP pool.
2. Enter the following for Option 43: e2 04 0a 10 e7 83

Value	Description
e2 04	vendor ID prefix (e2 is the hexadecimal value of the code 226 used to identify sub-option EXTREME.cloudiq-ip and 04 the hexadecimal value of the length of an IP address in bytes)
0a 10 e7 83	IP address 10.16.231.131 converted to hexadecimal

Segmented Management Instance Interface Types

The Management Instance supports the following interface types:

- Management Instance CLIP
  - You can assign a circuitless management IP (CLIP) address bound to a VRF.
  - The IP address is not bound to a physical network; it does not transmit nor receive IPv4 Address Resolution Protocol (ARP) or IPv6 Neighbor Discovery (ND) messages.
  - You do not need to configure a default or static route. This interface type uses all routing information learned by protocols attached to the VRF.
  - Packets can ingress on any port or VLAN in the VRF. You can configure accept policies to access the Management Instance CLIP from other VRF. Inter-VRF access is not permitted with traditional IP routing using OSPF, BGP, or RIP. Packets ingressing the switch from a VLAN belonging to a different VRF without a configured accept policy will not reach the Management Instance CLIP IP address.

    - You can use this interface type for CLIP management network routing in a Fabric network or Layer 3 routing network.

- Management Instance OOB
    - You can assign a management IP address bound to the Out-of-Band (OOB) interface.
    - The Dynamic Host Configuration Protocol (DHCP) Client can request an IPv4 address for the Management Instance OOB interface.
    - You must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link networks.
    - You can use this interface type for OOB management network routing, as an alternative to in-band network routing management.
- Management Instance VLAN
    - You can assign a Management Instance IP address to an inband VLAN.
    - The DHCP Client can request an IPv4 address for the Management Instance VLAN interface.
    - The interface resides on the physical VLAN segment, behaving as a host for sending and receiving IPv4 ARP and IPv6 ND messages.
    - You must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link (other subnets) networks.
    - No internal routing occurs between other non Management Instance VLANs. Packets must ingress on one of the ports in the VLAN.
    - You can use the Management Instance VLAN for management network routing, such as binding the Management Instance VLAN to an I-SID, which routes all management traffic to a single I-SID in a Fabric network. Also, other normal VLAN related operations such as VLAN port member changes are valid.

You can create only one of each interface type.

Segmented Management Instance Considerations and Restrictions

This section identifies considerations and restrictions for the Segmented Management Instance.

You can configure a maximum of three Management Instance interfaces, one of each type; an Out-of-Band (OOB) management interface, a Circuitless IP (CLIP) management interface, and a VLAN management interface.

You can configure the route priority for the Segmented Management Instance. The Source IP default route priority is management CLIP (weight 100), then management VLAN (weight 200), then management OOB interface (weight 300). You can route packets through a different management interface than the default configuration, but you must add a specific static route or change the default weight of the management interface.

Note:

If you change the default route weight, the management interface with the lowest weight value becomes the default route for all segmented management interface traffic.

Note:

The VSP 8600 Series Segmented Management Instance does not support ACL based filters or use of ping with -Q option to change the internal priority of management traffic.

You can configure the default topology IP for LLDP and SONMP advertisements. Both LLDP and SONMP advertise the same topology IP. SONMP supports only IPv4 addresses. If multiple IPv4 addresses are configured on an OOB or VLAN management interface, the advertised IP priority is static IP address, then DHCP IP address, then link-local IP address.

IPSec is not supported on Segmented Management Instance management interfaces.

DHCP Client for Segmented Management Instance

DHCP Client for the Segmented Management Instance supports IPv4 addresses only, and cannot be enabled on multiple management interfaces simultaneously. The DHCP Client only supports the in-band VLAN management interface, or the OOB management interface, or to cycle requests on the the VLAN then OOB management interface until an IP address is obtained on one of the interfaces.

Note:

The DHCP Client is disabled by default on previously configured or upgraded switches.

The DHCP Client is enabled by default in cycle mode when:

- The switch ships directly from manufacturing with VOSS Release 8.1.60 or later.

  The primary and secondary configuration file is not on the switch.

  The primary and secondary configuration file fail to load on the switch.

The DHCP Client is not available if RMON2 is configured on a Management Instance, and RMON2 is not available if the DHCP Client is configured on a Management Instance.

When DHCP is enabled on a Management Instance interface, the DHCP Client initial broadcast discovery packet and initial response from the DHCP server are not counted or shown in KHI management statistics for the management interface. Only the packets after the DHCP IP address assignment completes are counted and shown. After an IP address is assigned, a UDP socket opens and packets are counted on the interface.

If you change the DHCP Client configuration between management VLAN, OOB, or cycle, the default route provided by the DHCP server might delete and add with a different nexthop or network. DHCP Client configuration changes can cause interruptions to existing management connections.

DHCP static routes are not saved in the configuration file or displayed in **`show running-config`**. You can view DHCP static routes with **`show mgmt ip route static`**. If the DHCP Client adds a default route to an interface, the previous default route is deleted. If you modify a default route created by the DHCP Client, the route type output of **`show mgmt ip route static`** changes from DHCP to STATIC. You can save the modified to static default route to the configuration file, but on reboot the DHCP Client deletes the modified default route and restores the default static route the DHCP server specifies.

OOB Management Instance

Note:

OOB Management Instance is not supported on VSP 8600 Series or XA1400 Series.

You can associate only one OOB interface with an OOB Management Instance IP address.

You must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link networks.

You can only configure Layer 3 networking parameters in `mgmt OOB` interface CLI mode. You can only configure Layer 1 and Layer 2 networking parameters in `interface mgmtEthernet mgmt` CLI mode.

CLIP Management Instance

You can associate only one VRF ID with a CLIP Management Instance IP address.

You must configure a new loopback interface `isis ip-source address` if you migrate the current ISIS IP address to the CLIP Management Instance when the IP address is the same as a previously configured IP shortcut.

Advertisement of the IPv4 or IPv6 address in the GRT for the CLIP Management Instance to ISIS occurs automatically. Advertisement of the IPv4 or IPv6 address in the VRF Layer 3 VSN bound to the CLIP Management Instance occurs automatically. You must configure route redistribution to advertise the CLIP Management Instance to different protocols.

You must configure accept policies or configure inter-VRF route redistribution to access the CLIP Management Instance from a different VRF.

Packets sent to the CLIP Management Instance IP address must ingress the switch from a VLAN associated with the VRF associated with the CLIP Management Instance.

UDP server applications such as TFTP or RADIUS dynamic server or SMMP can have limitations when multiple Segmented Management Instances are configured with overlappping or asymmetrical routing:

Note:

The limiations listed do not apply to TCP applications or if a single Management Instance is configured.

- Client communication to the CLIP Management Instance IP address is from the same subnet as the VLAN Management Instance.
- Client communication to the CLIP Management Instance IP address when specific static routes or default route with higher preference back to the client network exist on OOB Management Instance or VLAN Management Instance.

- Client communication to the OOB Management Instance IP address or VLAN Management Instance IP address that relies on a default route with a lower preference than the internal default route used by the CLIP Management Instance.

Asymmetrical routing can occur in any of these three scenarios. For the first two scenarios you can use the OOB or VLAN Management Instance IP address instead of the CLIP Management Instance IP address. Also, use FTP or SCP file transfer as an alternative since those protocols are TCP based.

The third scenario, you can configure more specific static routes for networks originating UDP client communication to the OOB or VLAN Management Instance IP address if the CLIP Management Instance is also configured.

VLAN Management Instance

✳ **Note:**

VLAN Management Instance is not supported on VSP 8600 Series.

You can associate only one VLAN ID with a VLAN Management Instance IP address.

You must configure a default or static route to reach the next-hop gateway; no routing protocol information is used to access off-link networks.

For the VLAN Management Instance to take route priority when used in conjunction with the CLIP Management Instance, you must configure a default route for the VLAN Management Instance with a value lower than 100, or configure static routes for direct communication over the VLAN Management Instance and management networks.

Packets sent to the VLAN Management Instance IP address must ingress the switch from a VLAN port (or contain the VLAN ID) associated with the VLAN Management Instance. The system does not route packets between the VOSS routing VLAN and the VLAN Management Instance.

If you configure the same VLAN ID for VOSS routing and for the VLAN Management Instance, the VOSS routing stack transmits and receives all ARP, ND, and ICMP packets. In this scenario, the packets are only counted and shown in the VOSS routing KHI port statistics. The management statistics and KHI management statistics do not count or show the packets.

IPv4 and IPv6 address co-existence for both VOSS routing VLAN and VLAN Management Instance is supported, however you must manually match both IP address configurations between the VLANs. For example, the following configuration is not supported:

- VLAN Management Instance with both IPv4 and IPv6 address routing but only the IPv4 or IPv6 address configured for VOSS routing VLAN.

If you configure the VLAN Management Instance with a manual IPv4 address and a DHCP IPv4 address first, you cannot add a IPv4 address to a VOSS routing VLAN.

If you configure the VLAN Management Instance with an IPv6 address first, you can only add one IPv6 global address to a VOSS routing VLAN.

Configuration Example - Coexistence with Port-Based VLAN

The following example shows how the VLAN Management Instance can be configured to share the same IP address as a routing port-based VLAN.

You can configure the VOSS VLAN first and then configure the VLAN Management Instance or vice versa. You can remove or readd the coexistence at anytime.

Note:

With the coexistence between VOSS routing stack and the VLAN Management Instance, packets sent to the VLAN Management Instance IP address must ingress the switch from a VLAN port (or contain the VLAN ID) associated with the VLAN Management Instance. The system does not route packets between the VOSS routing VLAN and the VLAN Management Instance.

Example

IPv4

```
vlan create 10 type port-mstprstp 0
vlan members add 10 1/1
interface vlan 10
ip address 192.0.2.0/24
exit
mgmt vlan 10
ip address 192.0.2.0/24
ip route 0.0.0.0/0 next-hop 192.0.2.1
enable
```

IPv6

```
vlan create 10 type port-mstprstp 0
vlan members add 10 1/1
interface vlan 10
ipv6 interface address 2001:DB8::/32
ipv6 interface enable
exit
mgmt vlan 10
ipv6 address 2001:DB8::/32
ipv6 route 0::0/0 next-hop 2001::1
enable
```

Configuration Example - Coexistence with Brouter Port

The following example shows how the VLAN Management Instance can be configured to share the same IP address as a brouter interface.

You must configure the brouter interface before you enable the VLAN Management Instance. When the VLAN Management Instance is enabled, you must disable the VLAN Management Instance before you disable the brouter port.

Example

IPv4

```
interface GigabitEthernet 1/1
no shutdown
brouter port 1/1 vlan 10 subnet 192.0.2.0/24
```

```
mgmt vlan 10
ip address 192.0.2.0/24
enable
```

IPv6

```

interface GigabitEthernet 1/1
no shutdown
ipv6 interface vlan 10
ipv6 interface address 2001:DB8::/32
ipv6 interface enable
mgmt vlan 10
ipv6 address 2001:DB8::/32
enable
```

Considerations and Restrictions

The following considerations and restrictions apply when a VLAN Management Instance coexists with a port-based VLAN or with a brouter port.

- If you want a dual stack IPv4 and IPv6 coexistence between VOSS and VLAN Management Instance, you must configure the same IPv4 and IPv6 addresses on the VLAN Management Instance and on the VOSS VLAN.

  You cannot configure VLAN Management Instance with both IPv4 and IPv6 and configure the VOSS VLAN with IPv4 or IPv6 only.
- If you disable VOSS routing for IPv4, then you must disable routing for IPv6, and vice versa.

Segmented Management Instance Configuration using the CLI

This section provides procedures to configure segmented management instance using the command line interface (CLI).

Create a Segmented Management Instance

You must create a Management Instance to gain access to specific management applications. After you create the Management Instance, you can add an IP address to it and configure route redistribution to advertise reachability of the Management Instance to the rest of the network.

About this task

The Management Instance supports different management interface types. When you create the Management Instance, you specify the interface type and the switch automatically creates the appropriate instance ID for that type.

A management VLAN is recommended for Layer 2 deployments. In a Layer 3 routing or Fabric deployment, use a management CLIP. For Out-of-band Management, use a management OOB.

Each Management Instance supports a IPv4 and IPv6 (global scope) management address for use by management applications.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Create the Management Instance required for your deployment:

   a. To create a management CLIP:

   ```
   mgmt clip [vrf WORD<1-16>]
   ```

   Note:

   If you do not specify a VRF, the management CLIP uses the GRT. You cannot use mgmtrouter as the VRF.

   OR

   b. To create a management OOB:

   ```
   mgmt oob
   ```

   OR

   c. To create a management VLAN and associate it with an existing port-based VLAN:

   ```
   mgmt vlan <2-4059>
   ```

3. Enable the Management Instance:

   ```
   enable
   ```

Example

Create and enable a Management CLIP:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt clip
Switch:1(mgmt:clip)#enable
```

Create and enable a Management OOB:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt oob
Switch:1(mgmt:oob)#enable
```

Create and enable a Management VLAN:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt vlan 20
Switch:1(mgmt:vlan)#enable
```

Delete a Segmented Management Instance

Use this task to delete a Management Instance. Deleting the Management Instance removes the IP address, and changes the associated VRF for a management CLIP.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Delete the Management Instance:

   `no mgmt {clip | oob | vlan}`

Configure the DHCP Client for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to configure the DHCP Client to obtain an IPv4 address for the Management Instance VLAN interface or Out-of-Band interface.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enable and configure the DHCP Client for a management interface:

   `mgmt dhcp-client {cycle | oob | vlan}`

3. Disable and clear the DHCP Client configuration for a management interface:

   `no mgmt dhcp-client`

Example

The following example configures the DHCP Client to cycle IPv4 requests for the In-Band management VLAN interface, and then the management OOB interface. The system cycles attempts until one management interface receives an IP address from the DHCP server:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt dhcp-client cycle
```

Variable Definitions

The following table defines parameters for the **`mgmt dhcp-client`** command.

Variable	Value
cycle	DHCP Client cycles IP requests for in-band VLAN and Out-of-Band management interfaces.
oob	DHCP Client requests an IP address for the Out-of-Band management interface.

Table continues…

Variable	Value
vlan	DHCP Client requests an IP address for the VLAN management interface.

Configure an IP Address for a Segmented Management Instance

Use this task to add an IPv4 or IPv6 address to a Management Instance.

Before you begin

- Ensure the IP address you plan to assign is not in use by an existing VLAN or CLIP IP subnet configured on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the configuration mode for the Management Instance:

   ```
   mgmt {clip | oob | vlan}
   ```

3. Add an IPv4 address:

   ```
   ip address {A.B.C.D [A.B.C.D] | A.B.C.D/X}
   ```

4. Add an IPv6 address:

   ```
   ipv6 address WORD<0-255>
   ```

Example

Add an IPv4 address to the VLAN Management Instance:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt vlan
Switch:1(mgmt:vlan)#ip address 192.0.2.12/24
```

Add an IPv4 address to the OOB Management Instance:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt oob
Switch:1(mgmt:oob)#ip address 192.0.2.12 255.255.255.0
```

Add an IPv6 address to the CLIP Management Instance:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt clip
Switch:1(mgmt:clip)#ipv6 address 2001:DB8::1/128
```

Configure a Segmented Management Instance Interface as Default Topology IP

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to configure a Management Instance with a default topology IP.

Note:

You can only configure one Management Instance interface as the default topology IP.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enter the configuration mode for the Management Instance:

   `mgmt {clip | oob | vlan}`

3. Configure the Management Instance as the default topology IP.

   `force-topology-ip`

Example

The following example configures the Segmented Management Instance VLAN as the default topology IP:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt vlan
Switch:1(mgmt:vlan)#force-topology-ip
```

Configure Static Routes for a Management Instance

Use this task to configure static routes for Management Instances.

Note:

Up to 100 IPv4 and IPv6 static routes can be configured.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enter the configuration mode for the Management Instance:

   `mgmt {clip | oob | vlan}`

3. **(Optional)** Configure a static route:

   ```
   ip route <A.B.C.D A.B.C.D | A.B.C.D/X> next-hop <A.B.C.D> [weight
   <1-65535>]
   ```

   OR

   ```
   ipv6 route WORD<0-255> [next-hop WORD<0-255>] [weight <1-65535>]
   ```

Example

Add a static route to configure routing for a Management Instance:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt vlan
Switch:1(mgmt:vlan)#ip route 192.0.2.2/24 next-hop 198.51.100.1
```

Variable definitions

The following table defines parameters for the **`ip route`** and **`ipv6 route`** commands.

Variable	Value
<A.B.C.D A.B.C.D | A.B.C.D/X>	Specifies the IP address and mask in one of the following formats: • A.B.C.D A.B.C.D • A.B.C.D/X
next-hop <A.B.C.D> or next-hop WORD<0-255>	Specifies the next hop address for the static route. Use an IP in the same subnet as the management VLAN IP address.
weight <1–65535>	Specifies the static route cost. The default is 100 for CLIP, 200 for VLAN, and 300 for OOB. The management CLIP uses an internal static route with a weight of 100. If you use both CLIP and VLAN and need to force all default traffic out the management VLAN interface, configure a default static route with a weight lower than 100.
WORD<0-255>	Specifies the IPv6 address.

Configure MAC-offset for a Management VLAN Instance

Use this task to configure MAC-offset for a Management VLAN instance.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the MAC-offset for a Management VLAN instance:

```
mgmt vlan mac-offset <MAC-offset>
```

Note:

Different hardware platforms support different ranges.

Example

Configure the MAC-offset for the Management VLAN instance:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#mgmt vlan
Switch:1(mgmt:vlan)#mac-offset <0-511>
```

Variable Definitions

The following table defines parameters for the **`mgmt vlan`** interface.

Variable	Value
mac-offset <*MAC-offset*>	Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

Migrate a VLAN or CLIP IP address to the Segmented Management Instance

Use this procedure to designate an existing VLAN or loopback IP address to the Segmented Management Instance during an upgrade. This action moves the IP interface from the VOSS routing stack to the management stack to use with management applications.

About this task

Note:

Do not migrate interfaces used for routing purposes, for example, where you configure Layer 3 routing protocols.

This command does not apply to the OOB or mgmtEthernet interface. Releases that support this migration procedure automatically move the IP address on the mgmtEthernet interface from the routing stack to the Segmented Management Instance during the upgrade to this release.

Procedure

1. Enter Interface Configuration mode for either a VLAN or loopback interface:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   `interface vlan <1-4059>` or `interface loopback <1-256>`

2. Select the interface address for migration:

```
migrate-to-mgmt
```

3. View the designated interface addresses selected for migration:

   ```
   show mgmt migration
   ```

4. Save the configuration selected for migration:

   ```
   save config
   ```

Example

Identify an IP address currently assigned to an inband VLAN to migrate to the Management VLAN. The example assumes you already identified a CLIP address. The VRF column in **`show mgmt migration`** indicates where the interface is being moved from.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface vlan 20
Switch:1(config-if)#migrate-to-mgmt
Switch:1(config-if)#show mgmt migration

=============================================================================
                                    Mgmt Migration Information
=============================================================================
IFINDEX   DESCR      VRF            IPV4                 IPV6
-----------------------------------------------------------------------------
1344      CLIP-1     GlobalRouter   192.0.2.102/32       10:0:0:0:0:0:0:1/128
2068      VLAN-20    GlobalRouter   198.51.100.6/24      20:0:0:0:0:0:0:1/64

2 out of 2 Total Num of mgmt migrate entries displayed
-----------------------------------------------------------------------------

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

View Segmented Management Instance Information

Use this task to view Management Instance information.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View general configuration information:

   ```
   show mgmt interface [clip | oob | vlan]
   ```

3. View operational routes for the Management Instance:

   ```
   show mgmt ip route [clip | oob | vlan]
   ```

   OR

   ```
   show mgmt ipv6 route [clip | oob | vlan]
   ```

   Note:

   Routes with a type of LOCAL have a metric equal to 1.

4. View configured static routes for the Management Instance:

```
show mgmt ip route static [vlan | oob | clip]
```

OR

```
show mgmt ipv6 route static [vlan | oob | clip]
```

Note:

Routes with a type of LOCAL have a metric equal to 256.

5. View the ARP or Neighbor Discovery cache information for the Management Instance:

   ```
   show mgmt ip arp [clip | oob | vlan]
   ```

   OR

   ```
   show mgmt ipv6 neighbor [clip | oob | vlan]
   ```

Example

```
Switch:1>show mgmt interface vlan
=====================================================================================
                                   Mgmt Interface Information
=====================================================================================
INST      DESCR      TYPE      ADMIN      VLAN      PORT      VRF            PHYSICAL
--------------------------------------------------------------------------------------
4         Mgmt-vlan  VLAN      enable     2         -                       192.0.2.188

1 out of 1 Total Num of mgmt interfaces displayed
------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ip route
==========================================================================================
                          Mgmt IPv4 Route Information - Table main
==========================================================================================
DEST/MASK            NEXTHOP              METRIC     INTERFACE       TYPE
------------------------------------------------------------------------------------------
0.0.0.0/0            0.0.0.0              100        Mgmt-clip       INTERNAL
0.0.0.0/0            0.0.0.0              300        Mgmt-oob1       DHCP
192.0.2.189/24       0.0.0.0              256        Mgmt-vlan       LOCAL
2 out of 2 Total Num of mgmt ip route displayed
------------------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ip route static
==========================================================================================
                     Mgmt IPv4 Static Route Information - Table main
==========================================================================================
INTERFACE       DEST/MASK            NEXTHOP              METRIC     STATE     TYPE
------------------------------------------------------------------------------------------
Mgmt-vlan       192.0.2.1/24         10.0.0.30            200        ACTIVE    STATIC
Mgmt-vlan       198.51.100.5/24      10.0.0.40            200        ACTIVE    STATIC
Mgmt-oob1       0.0.0.0/0            192.0.2.5            300        ACTIVE    DHCP
```

```
Switch:1>show mgmt ipv6 route static
==========================================================================================
                     Mgmt IPv6 Static Route Information - Table main
==========================================================================================
INTERFACE       DEST/MASK            NEXTHOP              METRIC     STATE
------------------------------------------------------------------------------------------
-
Mgmt-vlan       40:0:0:0:0:0:0:0/64  10:0:0:0:0:0:0:40     200       ACTIVE
Mgmt-vlan       50:0:0:0:0:0:0:0/64  10:0:0:0:0:0:0:50     200       ACTIVE
```

```
Switch:1>show mgmt ip arp
==========================================================================================
```

```
            Mgmt IP ARP Information
==========================================================================================
IP_ADDRESS        INTERFACE    MAC_ADDRESS        STATE
------------------------------------------------------------------------------------------
-
10.10.10.1        Mgmt-vlan    00:1d:af:64:a2:14  REACHABLE
10.10.10.22       Mgmt-vlan    00:18:b0:5a:92:14  STALE
10.10.10.33       Mgmt-vlan    00:50:56:8c:43:55  FAILED
```

```
Switch:1>show mgmt ipv6 neighbor
==========================================================================================
            Mgmt IPv6 Neighbor Information
==========================================================================================
IPV6_ADDRESS    INTERFACE    MAC_ADDRESS          STATE
------------------------------------------------------------------------------------------
-
10::1           Mgmt-vlan    00:1d:af:64:a2:14    REACHABLE
10::22          Mgmt-vlan    00:18:b0:5a:92:14    STALE
10::33          Mgmt-vlan    00:50:56:8c:43:53    FAILED
```

View IP Address Information for a Segmented Management Instance

Use this task to view the IP address information for a Management Instance.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View Segmented Management Instance IP address information:

   `show mgmt ip [<clip | oob | vlan>]`

   OR

   `show mgmt ipv6 [<clip | oob | vlan>]`
3. View Segmented Management Instance topology IP address information:

   `show mgmt topology-ip`

Example

```
Switch:1>#show mgmt ip vlan

==========================================================================================
                                   Mgmt IP Information
==========================================================================================
INST      DESCR      IPV4                 IPV6 GLOBAL/PREFIX LENGTH IPV6 LINKLOCAL
------------------------------------------------------------------------------------------
4         Mgmt-vlan  192.0.2.12/24        0:0:0:0:0:0:0:0/0         0:0:0:0:0:0:0:0

1 out of 1 Total Num of mgmt ip displayed
------------------------------------------------------------------------------------------
```

```
Switch:1>)#show mgmt topology-ip

==========================================================================================
                               Mgmt Topology IP Information
==========================================================================================
IPv4:
        Address: 192.0.2.10
        Instance: 1
        Description: oob1
```

```
IPv6:
        No address to display

Force-topology-ip setting: none
```

View Segmented Management Instance Statistics

Use this task to view Management Instance statistics.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View general Segmented Management Instance statistics:

   ```
   show mgmt statistics [clip | oob | vlan]
   ```

3. View ICMP statistics for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip icmp-statistics
   ```

   OR

   ```
   show mgmt ipv6 icmp-statistics
   ```

4. View IP statistics for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip ip-statistics
   ```

   OR

   ```
   show mgmt ipv6 ip-statistics
   ```

5. View the TCP connections for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip tcp-connections
   ```

   OR

   ```
   show mgmt ipv6 tcp-connections
   ```

6. View the TCP statistics for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip tcp-statistics
   ```

OR

```
show mgmt ipv6 tcp-statistics
```

7. View the UDP endpoints for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip udp-endpoints
   ```

   OR

   ```
   show mgmt ipv6 udp-endpoints
   ```

8. View the UDP statistics for the Management Instance:

   Note:

   This step does not apply to VSP 8600 Series.

   ```
   show mgmt ip udp-statistics
   ```

   OR

   ```
   show mgmt ipv6 udp-statistics
   ```

Example

```
Switch:1>show mgmt statistics

============================================================================================
======================================
                                                 Mgmt Interface Stats Information
============================================================================================
======================================
INST   DESCR       RX-PKTS             RX-ERROR            RX-DROP             TX-
PKTS             TX-ERROR            TX-DROP
--------------------------------------------------------------------------------------------
--------------------------------------
1      Mgmt-oob1   111667              0                   0
21412               0                   0

1 out of 1 Total Num of mgmt interfaces displayed
--------------------------------------------------------------------------------------------
--------------------------------------
```

```
Switch:1>show mgmt ip icmp-statistics

==================================================================================
                        Mgmt ICMP Statistics Information
==================================================================================
InMsgs           : 44
InErrors         : 0
InCsumErrors     : 0
InDestUnreachs   : 44
InTimeExcds      : 0
InParmProbs      : 0
InSrcQuenchs     : 0
InRedirects      : 0
InEchos          : 0
InEchoReps       : 0
InTimestamps     : 0
```

```
InTimestampReps  : 0
InAddrMask       : 0
InAddrMaskReps   : 0
OutMsgs          : 53
OutErrors        : 0
```

```
Switch:1>show mgmt ipv6 icmp-statistics

================================================================================
                       Mgmt ICMPv6 Statistics Information
================================================================================
InMsgs                    : 58
InErrors                  : 0
InCsumErrors              : 0
InDestUnreachs            : 0
InTimeExcds               : 0
InParmProbs               : 0
InPktTooBigs              : 0
InRedirects               : 0
InEchos                   : 0
InEchoReps                : 0
InGroupMembQueries        : 0
InGroupMembReductions     : 0
InRouterSolicits          : 0
InRouterAdvertisements    : 55
InNeighborSolicits        : 0
InNeighborAdvertisements  : 3
InMLDv2Reports            : 0
InType134                 : 55
InType136                 : 3
OutMsgs                   : 69
OutErrors                 : 0
OutDestUnreachs           : 0
OutTimeExcds              : 0
OutParmProbs              : 0
OutPktTooBigs             : 0
OutRedirects              : 0
OutEchos                  : 0
OutEchoReps               : 0
OutGroupMembQueries       : 0
OutGroupMembResponses     : 0
OutGroupMembReductions    : 0
OutRouterSolicits         : 0
OutRouterAdvertisements   : 0
OutNeighborSolicits       : 13
OutNeighborAdvertisements : 0
OutMLDv2Reports           : 56
OutType133                : 56
OutType135                : 13
OutType143                : 0

--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ip ip-statistics

================================================================================
                         Mgmt IP Statistics Information
================================================================================
InReceives        : 1231729
InHdrErrors       : 0
InAddrErrors      : 489
InUnknownProtos   : 0
InDiscards        : 0
InDelivers        : 1221886
OutRequests       : 1212585
```

```
OutDiscards       : 20
OutNoRoutes       : 0
ForwDatagrams     : 0
ReasmTimeout      : 0
ReasmReqds        : 0
ReasmOKs          : 0
ReasmFails        : 0
FragOKs           : 0
FragFails         : 0
FragCreates       : 0

--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ipv6 ip-statistics

================================================================================
                        Mgmt IPv6 Statistics Information
================================================================================
InReceives        : 226
InHdrErrors       : 0
InAddrErrors      : 0
InUnknownProtos   : 0
InDiscards        : 0
InDelivers        : 62
InTooBigErrors    : 0
InNoRoutes        : 0
InTruncatedPkts   : 0
InMcastPkts       : 224
InOctets          : 20556
InMcastOctets     : 20416
InBcastOctets     : 0
InNoECTPkts       : 226
InECT1Pkts        : 0
InECT0Pkts        : 0
InCEPkts          : 0
OutRequests       : 71
OutDiscards       : 0
OutNoRoutes       : 0
OutForwDatagrams  : 0
OutMcastPkts      : 69
OutOctets         : 5412
OutMcastOctets    : 5272
OutBcastOctets    : 0
ReasmTimeout      : 0
ReasmReqds        : 0
ReasmOKs          : 0
ReasmFails        : 0
FragOKs           : 0
FragFails         : 0
FragCreates       : 0

--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ip tcp-connections

==========================================================================================
========================================
                                                     Mgmt IP TCP connections
==========================================================================================
========================================
STATE            RECV-Q     SEND-Q     Local Address:Port                            Peer
Address:Port
------------------------------------------------------------------------------------------
----------------------------------------
LISTEN           0          5          0.0.0.0:ftp
```

```
0.0.0.0:*
LISTEN           0          5          0.0.0.0:telnet
0.0.0.0:*
LISTEN           0          40         0.0.0.0:https
0.0.0.0:*
LISTEN           0          1          0.0.0.0:login
0.0.0.0:*
ESTAB            0          0          192.0.2.10:https
198.51.100.1:50694
ESTAB            0          3          192.0.2.10:telnet
198.51.100.1:58862
ESTAB            0          0          192.0.2.10:https
198.51.100.1:59774
------------------------------------------------------------------------------------------
----------------------------------------
```

```
Switch:1>show mgmt ipv6 tcp-connections

==========================================================================================
========================================
                                                    Mgmt IPv6 TCP connections
==========================================================================================
========================================
STATE            RECV-Q     SEND-Q     Local Address:Port                            Peer
Address:Port
------------------------------------------------------------------------------------------
----------------------------------------
LISTEN           0          5          *:ftp                                         *:*
LISTEN           0          5          *:telnet                                      *:*
LISTEN           0          40         *:https                                       *:*
LISTEN           0          1          *:login                                       *:*
------------------------------------------------------------------------------------------
----------------------------------------
```

```
Switch:1>show mgmt ip tcp-statistics

================================================================================
                Mgmt Combined IPv4/v6 TCP Statistics Information
================================================================================
TcpActiveOpens    : 9571
TcpPassiveOpens   : 9658
TcpAttemptFails   : 17
TcpEstabResets    : 86
TcpInSegs         : 1207867
TcpOutSegs        : 1199088
TcpRetransSegs    : 42
TcpInErrs         : 0
TcpOutRsts        : 89
TcpInCsumErrors   : 0
--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ipv6 tcp-statistics

================================================================================
                Mgmt Combined IPv4/v6 TCP Statistics Information
================================================================================
TcpActiveOpens    : 9626
TcpPassiveOpens   : 9713
TcpAttemptFails   : 17
TcpEstabResets    : 86
TcpInSegs         : 1212159
TcpOutSegs        : 1203293
TcpRetransSegs    : 42
TcpInErrs         : 0
```

```
TcpOutRsts        : 89
--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ip udp-endpoints

==========================================================================================
========================================
                                                      Mgmt IP UDP endpoints
==========================================================================================
========================================
STATE            RECV-Q     SEND-Q     Local Address:Port                            Peer
Address:Port
------------------------------------------------------------------------------------------
----------------------------------------
UNCONN           0          0          0.0.0.0:bootpc
0.0.0.0:*
UNCONN           0          0          0.0.0.0:tftp
0.0.0.0:*
UNCONN           0          0          192.0.2.10:ntp
0.0.0.0:*
UNCONN           0          0          0.0.0.0:ntp
0.0.0.0:*
UNCONN           0          0          0.0.0.0:snmp
0.0.0.0:*
------------------------------------------------------------------------------------------
----------------------------------------
```

```
Switch:1>show mgmt ipv6 udp-endpoints

==========================================================================================
========================================
                                                     Mgmt IPv6 UDP endpoints
==========================================================================================
========================================
STATE            RECV-Q     SEND-Q     Local Address:Port                            Peer
Address:Port
------------------------------------------------------------------------------------------
----------------------------------------
UNCONN           0          0          [0:0:0:0:0:0:0:1]:domain                      *:*
UNCONN           0          0          *:tftp                                        *:*
UNCONN           0          0          [fe80:0:0:0:f66e:95ff:fe9f:81]:ntp            *:*
UNCONN           0          0          [fe80:0:0:0:f66e:95ff:fe9f:a5]:ntp            *:*
UNCONN           0          0          [fe80:0:0:0:a8bb:ccff:fedd:ee01]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:fce7:79ff:fe04:999c]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:609a:4aff:fe4e:cf04]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:c482:2aff:fe75:2e66]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:c80a:73ff:fe00:364e]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:80cc:e9ff:fec7:b9e2]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:64da:41ff:fec5:489e]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:f8d7:d6ff:feda:62bc]:ntp          *:*
UNCONN           0          0          [fe80:0:0:0:f66e:95ff:fe9f:0]:ntp             *:*
UNCONN           0          0          [0:0:0:0:0:0:0:1]:ntp                         *:*
UNCONN           0          0          *:ntp                                         *:*
UNCONN           0          0          *:snmp                                        *:*

------------------------------------------------------------------------------------------
----------------------------------------
```

```
Switch:1>show mgmt ip udp-statistics

================================================================================
                         Mgmt UDP Statistics Information
================================================================================
UdpInDatagrams    : 63622
UdpNoPorts        : 44
UdpInErrors       : 0
```

```
UdpOutDatagrams   : 63666
UdpIgnoredMulti   : 0
UdpRcvbufErrors   : 0
UdpSndbufErrors   : 0
UdpInCsumErrors   : 0
--------------------------------------------------------------------------------
```

```
Switch:1>show mgmt ipv6 udp-statistics

================================================================================
                        Mgmt UDP6 Statistics Information
================================================================================
Udp6InDatagrams    : 0
Udp6NoPorts        : 0
Udp6InErrors       : 0
Udp6OutDatagrams   : 0
Udp6IgnoredMulti   : 0
Udp6RcvbufErrors   : 0
Udp6SndbufErrors   : 0
Udp6InCsumErrors   : 0
--------------------------------------------------------------------------------
```

Redistribution of CLIP Segmented Management Instance Examples

The CLIP Management Instance is added as a LOCAL route in the Control Processor Route Table Manager table and change list infrastructure. Existing route redistribution mechanisms redistribute local routes into the desired routing protocols within the associated VRF or across VRF instances.

Redistribute IPv4 CLIP Management Instance to OSPF in GRT

```
router ospf
redistribute direct
redistribute direct enable
exit
ip ospf apply redistribute direct
```

Redistribute IPv6 CLIP Management Instance to OSPF in GRT

```
router ospf
ipv6 redistribute direct
ipv6 redistribute direct enable
ipv6 ospf apply redistribute direct
```

Redistribute IPv4 CLIP Management Instance to OSPF in VRF

```
router vrf red
ip ospf redistribute direct
ip ospf redistribute direct enable
exit
ip ospf apply redistribute direct vrf red
```

Redistribute IPv6 CLIP Management Instance to OSPF in VRF

```
router vrf red
ipv6 ospf redistribute direct
ipv6 ospf redistribute direct enable
exit
ipv6 ospf apply redistribute direct vrf red
```

Redistribute IPv4 CLIP Management Instance to BGP in GRT

```
router bgp
redistribute direct
redistribute direct enable
ip bgp apply redistribute direct
```

Redistribute IPv6 CLIP Management Instance to BGP in GRT

```
router vrf
redistribute ipv6-direct
redistribute ipv6-direct enable
ipv6 bgp apply redistribute direct
```

Redistribute IPv4 CLIP Management Instance to BGP in VRF

```
router vrf red
ip bgp redistribute direct
ip bgp redistribute direct enable
exit
ip bgp apply redistribute direct vrf red
```

Redistribute IPv6 CLIP Management Instance to BGP in VRF

```
router vrf red
ip bgp redistribute ipv6-direct
ip bgp redistribute ipv6-direct enable
exit
ipv6 bgp apply redistribute direct vrf red
```

Accept Policy for IPv4 CLIP Management Instance in GRT to VRF Red (I-SID 200)

```
#grt-->vrf
router vrf red
isis accept i-sid 0
isis accept i-sid 0 enable
isis redistribute direct
isis redistribute direct enable
exit
isis apply accept vrf red
isis apply redistribute direct vrf red

#vrf-->grt
router isis
accept i-sid 200
accept i-sid 200 enable
exit
isis apply accept
```

Accept Policy for IPv6 CLIP Management Instance in GRT to VRF Red (I-SID 200)

```
#grt-->vrf
router vrf red
ipv6 isis accept i-sid 0
ipv6 isis accept i-sid 0 enable
ipv6 isis redistribute direct
ipv6 isis redistribute direct enable
exit
ipv6 isis apply accept vrf red
ipv6 isis apply redistribute direct vrf red

#vrf-->grt
router isis
ipv6 accept i-sid 200
ipv6 accept i-sid 200 enable
exit
ipv6 isis apply accept
```

Accept Policy for IPv4 CLIP Management Instance in VRF Blue (I-SID 300) to GRT

```
#vrf --> grt
router isis
accept i-sid 300
accept i-sid 300 enable
```

```
redistribute direct
redistribute direct enable
exit
isis apply accept
isis apply redistribute direct

#grt --> vrf
router vrf blue
isis accept i-sid 0
isis accept i-sid 0 enable
exit
isis apply accept vrf blue
```

Accept Policy for IPv6 CLIP Management Instance in VRF Blue (I-SID 300) to GRT

```
#vrf --> grt
router isis
ipv6 accept i-sid 300
ipv6 accept i-sid 300 enable
ipv6 redistribute direct
ipv6 redistribute direct enable
exit
ipv6 isis apply accept
ipv6 isis apply redistribute direct

#grt --> vrf
router vrf blue
ipv6 isis accept i-sid 0
ipv6 isis accept i-sid 0 enable
exit
ipv6 isis apply accept vrf blue
```

Configure a Segmented Management Instance Using quick-config-mgmt Utility

Use the following procedure to run the quick-config-mgmt utility script to ease the transition to the Segmented Management Instance.

Note:

XA1400 Series does not support the OOB Management Instance.

Note:

Product Notice: quick-config-mgmt is not supported on VSP 8600 Series.

The quick-config-mgmt utility recognizes existing configuration. For the OOB Management Instance, you can overwrite the existing configuration only. However, for the VLAN Management Instance, you can overwrite the existing configuration, or you can migrate the existing configuration to a coexistence of IP on both VOSS VLAN and management VLAN.

The quick-config-mgmt utility supports the following:

- IPv4 only
- only one interface at one time
- Out-of-Band mangagement and In-Band VLAN management

About this task

You can use this procedure to help you transition to a new Segmented Management Instance. You can configure IPv4, static routes, and DHCP support for the Out-of-Band (OOB) Mangagement Instance or for the In-Band VLAN Management Instance. If configuration exists for the interface type you selected, you are prompted to replace the configured interface or to quit the utility.

Important:

If you configure DHCP, any other running DHCP instance is stopped and a new DHCP instance is created on the interface. This might cause loss of conectivity.

The default values are given in square brackets. You can input your values at the prompt or you can press `Enter` to accept the default values.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command to start the utility:

   ```
   quick-config-mgmt
   ```

   Important:

   If DHCP mode cycle is enabled, the following warning message displays to inform you that DHCP client will be disabled, if you continue.

   ```
   Continuing will disable dhcp and may affect your connectivity to
   the DUT. Do you want to continue? y/n [n]:
   ```

Example

The following examples show outputs from the **`quick-config-mgmt`** utility.

Configure the OOB Mangagement Instance:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.

 Once the basic parameters are configured, additional configuration can proceed using
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]:
 Please enter the Management Address IPv4 address, "d" for DHCP configuration or "q" to
quit [192.0.2.2]:
 Please enter the Management Address Mask IPv4 address or "q" to quit [255.255.255.0]:
 Please enter the Default Gateway Address IPv4 address, 0.0.0.0 for no default gateway,
or "q" to quit [192.0.2.5] :
 Management interface created successfully
```

Replace an existing OOB Mangagement Instance configuration:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.

 Once the basic parameters are configured, additional configuration can proceed using
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]:
 MGMT OOB is already configured.
 Continuing may remove parts or all of current config.
 Do you want to continue? y/n [y]:
 Please enter management interface type or "q" to quit. [1]:
 Please enter the Management Address IPv4 address, "d" for DHCP configuration or "q" to
quit [192.0.2.2]:
 Please enter the Management Address Mask IPv4 address or "q" to quit [255.255.255.0]:
 Please enter the Default Gateway Address IPv4 address, 0.0.0.0 for no default gateway,
or "q" to quit [192.0.2.5] :
 Management interface created successfully
```

Configure the In-band port-based VLAN Management Instance by removing parts of or all of the existing VLAN configuration:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.

 Once the basic parameters are configured, additional configuration can proceed using
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]: 3
 MGMT VLAN is already configured.
 Continuing may remove parts or all of current config.
 Do you want to continue? y/n [n]: y
 Please enter VLAN ID (2-4059) or "q" to quit [4059]: 2
 VLAN 2 is already in use.
 Do you want to re-use existing vlan configuration? y/n/q: [n]
 This option will remove all current config on VLAN 2.
 Please enter port to be added to the in-band management VLAN or "q" to quit [1/1]:
 Please enter the Management Address Mask IPv4 address or "q" to quit [255.255.255.0]:
 Please enter the Default Gateway Address IPv4 address, 0.0.0.0 for no default gateway,
or "q" to quit [192.0.2.5] :
 Management interface created successfully
```

Configure the In-band port-based VLAN Management Instance by reusing the existing VLAN configuration:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.

 Once the basic parameters are configured, additional configuration can proceed using
```

```
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]: 3
 MGMT VLAN is already configured.
 Continuing may remove parts or all of current config.
 Do you want to continue? y/n [n]: y
 Please enter VLAN ID (2-4059) or "q" to quit [4059]: 2
 VLAN 2 is already in use.
 Do you want to re-use existing vlan configuration? y/n/q: [y]
 Please enter port to be appended to the in-band management VLAN or leave empty
 to keep currently configured ports or "q" to quit []: 1/1
 Please enter the Management Address IPv4 address, "d" for DHCP configuration or "q" to
quit [192.0.2.2]:
 Please enter the Management Address Mask IPv4 address or "q" to quit [255.255.255.0]:
 Please enter the Default Gateway Address IPv4 address, 0.0.0.0 for no default gateway,
or "q" to quit [192.0.2.5] :
 Management interface created successfully
```

Configure the In-band port-based VLAN Management Instance by reusing the existing VLAN configuration when IP address is configured and coexistance of mgmt and routing on same VLAN is desired:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.

 Once the basic parameters are configured, additional configuration can proceed using
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]: 3
 MGMT VLAN is already configured.
 Continuing may remove parts or all of current config.
 Do you want to continue? y/n [n]: y
 Please enter VLAN ID (2-4059) or "q" to quit [4059]: 2
 VLAN 2 is already in use.
 Do you want to re-use existing vlan configuration? y/n/q: [y]
 Please enter port to be appended to the in-band management VLAN or leave empty
 to keep currently configured ports or "q" to quit []: 1/1
 IP address is already configured on VLAN 2.
 Do you want to configure co-existence of mgmt and routing on the same vlan? y/n/q: [y]
 Please enter the Management Address IPv4 address, "d" for DHCP configuration or "q" to
quit [192.0.2.2]:
 Please enter the Management Address Mask IPv4 address or "q" to quit [255.255.255.0]:
 Please enter the Default Gateway Address IPv4 address, 0.0.0.0 for no default gateway,
or "q" to quit [192.0.2.5] :
 Management interface created successfully
```

Configure the In-band port-based VLAN Management Instance by reusing the existing VLAN configuration when IP address is configured but coexistance of mgmt and routing on same VLAN is not desired:

```
Switch:1(config)#quick-config-mgmt
Welcome to the management interface setup utility.
You will be requested for information to initially configure the switch.
When finished the information will be applied and stored as a part of the
configuration.
```

```
 Once the basic parameters are configured, additional configuration can proceed using
other management interfaces.
 Press q to abort at any time.
 Management interface types:
    1 - Out of band management port
    3 - In-band port-based VLAN
 Please enter management interface type or "q" to quit. [1]: 3
 MGMT VLAN is already configured.
 Continuing may remove parts or all of current config.
 Do you want to continue? y/n [n]: y
 Please enter VLAN ID (2-4059) or "q" to quit [4059]: 2
 VLAN 2 is already in use.
 Do you want to re-use existing vlan configuration? y/n/q: [y]
 Please enter port to be appended to the in-band management VLAN or leave empty
 to keep currently configured ports or "q" to quit []: 1/1
 IP address is already configured on VLAN 2.
 Do you want to configure co-existence of mgmt and routing on the same vlan? y/n/q: [n]
 Management interface created successfully
```

Segmented Management Instance Configuration for VOSS using the EDM

Note:

This section does not apply to VSP 8600 Series.

This section provides procedures to configure segmented management instance using the EDM.

Configure a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

You must create a Management Instance to gain access to specific management applications.

About this task

The Management Instance supports different management interface types. When you create the Management Instance, you specify the interface type and the switch automatically creates the appropriate instance ID for that type.

In a Layer 2 routing deployment, use a management VLAN. In a Layer 3 routing or Fabric deployment, use a management CLIP. To separate management network from Layer 2 and Layer 3, use a management OOB.

Each Management Instance supports a IPv4 and IPv6 (global scope) management address for use by management applications.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.

4. Select the **Interface** tab.
5. Select **Insert**.
6. In the **InstanceId** field, select the type of Management Instance to create.
7. **(Optional)** For a CLIP Management Instance, in the **VrfName** field, type the VRF name to associate with the CLIP instance.

   Note:

   If you want to associate the GRT with the CLIP instance, type **GlobalRouter** in the **VrfName** field. You cannot use mgmtrouter as the VRF.
8. For a VLAN Management Instance, in the **VlanId** field, type the VLAN ID to associate the management VLAN with an existing port-based VLAN.
9. For an OOB Management Instance, in the **OOBIfindex** field, select the interface port number to associate for Out-of-Band management.
10. Select the **State** check box to enable the instance.
11. To specify the interface as the default topology IP for LLDP advertisements, select **InterfaceTopologyIpFlag**.
12. To administratively enable RMON for the interface, select **RmonAdminEnable**.
13. Select **Insert**.

Interface field descriptions

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

Name	Description
InstanceId	Indicates the Management Instance type associated with this entry.
InterfaceType	Indicates the interface type.
VlanId	Specifies the VLAN ID to associate with the management VLAN.
OOBIfindex	Specifices the interface ID to associate with the mangement OOB.
VrfName	Specifies the VRF name to associate with the management CLIP .
State	Indicates if the interface is enabled for this instance. The default is disabled.
InterfaceMacAddr	Indicates the MAC address for the interface.
InterfaceName	Indicates the interface name.
InterfaceTopologyIpFlag	Specifies if the interface is the default topology source IP.
ZtpOn	Identifies the Zero Touch Provisioning status for the interface.

Table continues…

Name	Description
RmonAdminEnable	Specifies if RMON is administrative enabled for the interface.
RmonOperEnable	Indicates the RMON operational status for the interface.
RmonIpAddress	Indicates the RMON IP address for the interface.
MacOffset	Translates the IP address into a MAC address.

Configure DHCP Client for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to configure a DHCP Client on a management interface.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **Dhcp** tab.
5. In the **Client** field, select an option to configure the DHCP Client.
6. Select **Apply**.

Dhcp Field Descriptions

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

Name	Description
Client	Specifies the DHCP client configuration: • **oob** - DHCP Client on the Out-of-Band management interface. • **vlan** - DHCP Client on the VLAN management interface. • **cycle** - DHCP Client cycles between in-band and Out-of-Band management interfaces until an IP address is obtained on one management interface. • **disable** - DHCP Client is disabled.
ClientPreferredInterface	Shows the DHCP Client preferred management interface when in cycle mode. On reboot, the system first attempts to aquire a DHCP IP address on the preferred interface.

View IPv4 ARP Information for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv4 Address Resolution Protocol (ARP) information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **IpArp** tab.

IpArp Field Descriptions

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

Name	Description
Address	Shows the IPv4 address of the ARP entry.
Instance	Shows the Management Instance ID.
IntfName	Shows the Management Instance interface name for the ARP entry.
MacAddr	Shows the MAC address for the ARP entry.
State	Shows the state of the ARP entry. The state can be one of the following: • reachable • stale • permanent • failed • delay

View IPv6 ND Information for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv6 Neighbor Discovery (ND) information.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.

4. Select the **Ipv6Neighbor** tab.

Ipv6Neighbor Field Descriptions

Use the data in the following table to use the Ipv6Neighbor tab.

Name	Description
Addr	Shows the IPv6 address of the neighbor entry.
Instance	Shows the Management Instance ID.
IntfName	Shows the Management Instance interface name for the neighbor entry.
MacAddr	Shows the MAC address for the neighbor entry.
State	Shows the state of the neighbor entry. The state can be one of the following: • reachable • stale • permanent • failed • delay

Configure IPv4 Static Routes for a Management VLAN

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to configure static routes for the management VLAN.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **IpStaticRoute** tab.
5. Select **Insert**.
6. For the **Instance**, select **vlan**.
7. Type the destination IP address and mask.
8. Type the next hop IP address.
9. Type a metric value.
10. Select **Insert**.

IpStaticRoute Field Descriptions

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

Name	Description
Instance	Specifies the Management Instance.
DestAddr	Specifies the destination IP address.
DestMask	Specifies the destination mask.
NextHop	Specifies the next hop address for the static route. Use an IP address in the same subnet as the management VLAN IP address.
IntfName	Specifies the Management Instance interface name for the route entry.
Metric	Specifies the static route cost. The default is 200. The management CLIP uses an internal static route with a weight of 100. If you use both CLIP and VLAN and need to force all default traffic out the management VLAN interface, configure a default static route with a weight lower than 100.
State	Shows if the route is active or inactive.

Configure IPv6 Static Routes for a Management VLAN

✱ **Note:**

This procedure does not apply to VSP 8600 Series.

Use this task to configure static routes for the management VLAN.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Expand **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **Ipv6StaticRoute** tab.
5. Select **Insert**.
6. For the **Instance**, select **vlan**.
7. Type the destination IPv6 address and prefix length.
8. Type the next hop IPv6 address.
9. Type a metric value.
10. Select **Insert**.

Ipv6StaticRoute Field Descriptions

Use the data in the following table to use the Ipv6StaticRoute tab.

Name	Description
Instance	Specifies the Management Instance.
DestAddr	Specifies the destination IP address.
DestPrefixLen	Specifies the destination prefix length.
NextHop	Specifies the next hop address for the static route. Use an IP address in the same subnet as the management VLAN IP address.
IntfName	Specifies the Management Instance interface name for the route entry.
Metric	Specifies the static route cost. The default is 200. The management CLIP uses an internal static route with a weight of 100. If you use both CLIP and VLAN and need to force all default traffic out the management VLAN interface, configure a default static route with a weight lower than 100.
State	Shows if the route is active or inactive.

View IPv4 Operational Routes for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv4 operational routes.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **IpRoute** tab.

IpRoute Field Descriptions

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

Name	Description
DestAddr	Shows the destination address of the route entry.
DestMask	Shows the destination mask of the route entry.
Metric	Shows the metric, or cost, assigned to the route entry. If multiple entries exist to the same destination, the metric determines which route is used. Routes with a type of LOCAL have a metric equal to 1.

Table continues…

Name	Description
Instance	Shows the Management Instance ID.
NextHop	Shows the next hop for the route entry.
IntfName	Shows the Management Instance interface name for the route entry.
Type	Shows the type of route entry.

View IPv6 Operational Routes for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv6 operational routes.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **Ipv6Route** tab.

Ipv6Route Field Descriptions

Use the data in the following table to use the Ipv6Route tab.

Name	Description
DestAddr	Shows the destination address of the route entry.
PrefixLen	Shows the destination prefix length of the route entry.
Metric	Shows the metric, or cost, assigned to the route entry. If multiple entries exist to the same destination, the metric determines which route is used. Routes with a type of LOCAL have a metric equal to 256.
Instance	Shows the Management Instance ID.
NextHop	Shows the next hop for the route entry.
IntfName	Shows the Management Instance interface name for the route entry.
Type	Shows the type of route entry.

Migrate an IP Address to a Segmented Management Instance

Note:

This procedure is not applicable for VOSS release 8.1.60 or later. You can only configure the migrate to management for a pre-existing VLAN or loopback management interface before you upgrade to this release.

Note:

This procedure does not apply to VSP 8600 Series.

Use this procedure to designate an existing VLAN or loopback IP address as a Segmented Management Instance. This action moves the IP interface from the VOSS routing stack to the management stack to use with management applications.

About this task

You cannot migrate interfaces used for routing purposes, for example, where you configure Layer 3 routing protocols.

This command does not apply to the OOB or mgmtEthernet interface. Releases that support this migration procedure automatically move the IP address on the mgmtEthernet interface from the routing stack to the Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **Migrate** tab.
5. Select **Insert**.
6. Select the instance type, either **clip** or **vlan**.
7. Specify the existing VLAN or loopback ID.
8. Select **Insert**.

Migrate field descriptions

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

Name	Description
InstanceId	Specifies the interface instance to migrate.
InterfaceIndex	Shows the interface index of the identified interface.
InterfaceType	Shows the interface type.
Description	Shows the interface description.
VlanId	Specifies the VLAN ID for a port-based VLAN.
LoopbackId	Specifies the loopback ID.

Table continues…

Name	Description
VrfName	Shows the VRF associated with the loopback interface.
IpAddress	Shows the IPv4 address to migrate.
IpMask	Shows the subnet mask for the IPv4 address.
Ipv6Address	Shows the IPv6 address to migrate.
Ipv6PrefixLength	Shows the prefix length for the IPv6 address.

View Topology IP for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view the default topology IP address for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **TopologyIp** tab.

TopologyIp Field Descriptions

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

Name	Description
AddrType	Shows the IP address type for the topology IP.
Addr	Shows the IP address for the topology IP.
InterfaceName	Shows the interface name of the identified interface for the topology IP.
InstanceId	Specifies the interface instance for the topology IP.

View IP Address for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv4 address information for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.

4. Select the **IpAddress** tab.

IpAddress Field Descriptions

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

Name	Description
InstanceId	Specifies the interface instance.
Address	Shows IPv4 address for the interface instance.
Mask	Specifies the subnet mask of the IP address.
AddrOrigin	Shows the IP address origin.
IntfName	Shows the interface name.

View IPv6 Address for a Segmented Management Instance

✱ **Note:**

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv6 address information for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Mgmt**.
4. Select the **Ipv6Address** tab.

Ipv6Address Field Descriptions

Use the data in the following table to use the Ipv6Address tab.

Name	Description
InstanceId	Specifies the interface instance.
Address	Shows IPv6 address for the interface instance.
PrefixLength	Specifies the prefix length for the IPv6 address.
AddrOrigin	Shows the IPv6 address origin.
IntfName	Shows the interface name.
DadStatus	Shows the IPv6 DAD status of the address.

View IP Address Statistics for a Segmented Management Instance

✱ **Note:**

This procedure does not apply to VSP 8600 Series.

Use this task to view IP address statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IP** tab.
5. To clear IP statistics, select **Clear Stats**.
6. To clear IP counters, select **Clear Counters**.

IP Field Descriptions

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

Name	Description
InReceives	Shows the inbound packet statistics.
InHdrErrors	Shows the inbound packets with header errors statistics.
InAddrErrors	Shows the inbound packets with address errors statistics.
InUnknownProtos	Shows the inbound packets with unknown protocols statistics.
InDiscards	Shows the inbound packets discarded statistics.
InDelivers	Shows the inbound packets delivered statistics.
OutRequests	Shows the outbound packet requests statistics.
OutDiscards	Shows the outbound packets discarded statistics.
OutNotRoutes	Shows the outbound packets with no routes statistics.
ForwDatagrams	Shows the forwarded datagram packets statistics.
ReasmTimeout	Shows the packet reassembly timeouts statistics.
ReasmReqds	Shows the packet reassembly requests statistics.
ReasmOKs	Shows the successfully reassembled packets statistics.
ReasmFails	Shows the failed reassembled packets statistics.
FragOKs	Shows the successfully fragmented packets statistics.
FragFails	Shows the failed fragmented packets statistics.
FragCreates	Shows the fragments created statistics.

View IPv6 Address Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series or XA1400 Series.

Use this task to view IPv6 address statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IPv6** tab.
5. To clear IP statistics, select **Clear Stats**.
6. To clear IP counters, select **Clear Counters**.

IPv6 Field Descriptions

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

Name	Description
InReceives	Shows the inbound packet statistics.
InHdrErrors	Shows the inbound packets with header errors statistics.
InAddrErrors	Shows the inbound packets with address errors statistics.
InUnknownProtos	Shows the inbound packets with unknown protocols statistics.
InDiscards	Shows the inbound packets discarded statistics.
InDelivers	Shows the inbound packets delivered statistics.
InTooBigErrors	Shows the inboud packets too big errors statistics.
InNoRoutes	Shows the inbound packets with no routes statistics.
InTruncatedPkts	Shows the inbound packets truncated statistics.
InMcastPkts	Shows the inbound multicast packets statistics.
InOctets	Shows the inbound octets statistics.
InMcastOctets	Shows the inbound multicast octets statistics.
InBcastOctets	Shows the inbound broadcast octets statistics
InNoECTPkts	Shows the inbound packets with no Explicit Congestion Notification (ECN) statistics.
InECT1Pkts	Shows the inbound packets with ECT(1) statistics.
InECT0Pkts	Shows the inbound packets with ECT(0) statistics.
InCEPkts	Shows the inbound packets with Congestion Ecountered (CE) statistics.
OutRequests	Shows the outbound packet requests statistics.
OutDiscards	Shows the outbound packets discarded statistics.

Table continues…

Name	Description
OutNoRoutes	Shows the outbound packets with no routes statistics.
OutForwDatagrams	Shows the forwarded datagram packets statistics.
OutMcastPkts	Shows the outbound multicast packets statistics.
OutOctets	Shows the outbound octets statistics.
OutMcastOctets	Shows the outbound multicast octets statistics.
OutBcastOctets	Shows the outpound broadcast octets statistics.
ReasmTimeout	Shows the packet reassembly timeouts statistics.
ReasmReqds	Shows the packet reassembly requests statistics.
ReasmOKs	Shows the successfully reassembled packets statistics.
ReasmFails	Shows the failed reassembled packets statistics.
FragOKs	Shows the successfully fragmented packets statistics.
FragFails	Shows the failed fragmented packets statistics.
FragCreates	Shows the fragments created statistics.

View IP ICMP Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IP ICMP statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IP-ICMP** tab.
5. To clear IP statistics, select **Clear Stats**.
6. To clear IP counters, select **Clear Counters**.

IP-ICMP Field Descriptions

Use the data in the following table to use the IP-ICMP tab.

Name	Description
InMsgs	Shows the inbound messages statistics.
InErrors	Shows the inbound errors statistics.

Table continues…

Name	Description
InCsumErrors	Shows the inbound checksum errors statistics.
InDestUnreachs	Shows the inbound destination unreachable statistics.
InTimeExcds	Shows the inbound time exceeded statistics.
InParmProbs	Shows the inbound parameter problems statistics.
InSrcQuenchs	Shows the inbound source quenchs statistics.
InRedirects	Shows the inbound redirects statistics.
InEchos	Shows the inbound echos statistics.
InEchoReps	Shows the inbound echo replies statistics.
InTimestamps	Shows the inbound timestamps statistics.
InTimestampsReps	Shows the inbound timestamp replies statistics.
InAddrMasks	Shows the inbound address masks statistics.
InAddrMaskReps	Shows the inbound address mask replies statistics.
OutMsgs	Shows the outbound messages statistics.
OutErrors	Shows the outbound errors statistics.
OutDestUnreachs	Shows the outbound destination unreachable statistics.
OutTimeExcds	Shows the outbound time exceeded statistics.
OutParmProbs	Shows the outbound parameter problems statistics.
OutSrcQuenchs	Shows the outbound source quenchs statistics.
OutRedirects	Shows the outbound redirects statistics.
OutEchos	Shows the outbound echos statistics.
OutEchoReps	Shows the outbound echo replies statistics.
OutTimestamps	Shows the outbound timestamps statistics.
OutTimestampReps	Shows the outbound timestamps replies statistics.
OutAddrMasks	Shows the outbound address masks statistics.
MsgInType0	Shows the inbound Type0 messages statistics.
MsgOutType8	Shows the outbound Type8 messages statistics.

View IPv6 ICMP Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view IPv6 ICMP statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.

3. Select **Stats**.
4. Select the **IPv6-ICMP** tab.
5. To clear IP statistics, select **Clear Stats**.
6. To clear IP counters, select **Clear Counters**.

IPv6-ICMP Field Descriptions

Use the data in the following table to use the IPv6-ICMP tab.

Name	Description
InMsgs	Shows the inbound messages statistics.
InErrors	Shows the inbound errors statistics.
InCsumErrors	Shows the inbound checksum errors statistics.
InDestUnreachs	Shows the inbound destination unreachable statistics.
InTimeExcds	Shows the inbound time exceeded statistics.
InParmProbs	Shows the inbound parameter problems statistics.
InPktTooBigs	Shows the inbound packets too big statistics.
InRedirects	Shows the inbound redirects statistics.
InEchos	Shows the inbound echos statistics.
InEchoReplies	Shows the inbound echo replies statistics.
InGroupMembQueries	Shows the inbound group member queries statistics.
InGroupMembResponses	Shows the inbound group member responses statistics.
InGroupMembReductions	Shows the inbound group member reductions statistics.
InRouterSolicits	Shows the inbound router solicits statistics.
InRouterAdvertisements	Shows the inbound router advertisements statistics.
InNeighborSolicits	Shows the inbound neighbor solicits statistics.
InNeighborAdvertisements	SHows the inbound neighbor advertisements statistics.
InMLDv2Reports	Shows the inbound MLDv2 reports statistics.
InType134	Shows the inbound type134 statistics.
InType136	Shows the inbound type136 statistics.
OutMsgs	Shows the outbound messages statistics.
OutErrors	Shows the outbound errors statistics.
OutDestUnreachs	Shows the outbound destination unreachable statistics.
OutTimeExcds	Shows the outbound time exceeded statistics.

Table continues…

Name	Description
OutParmProbs	Shows the outbound parameter problems statistics.
OutPktTooBigs	Shows the outbound packets too big statistics.
OutRedirects	Shows the outbound redirects statistics.
OutEchos	Shows the outbound echos statistics.
OutEchoReps	Shows the outbound echo replies statistics.
OutGroupMembQueries	Shows the outbound group member queries statistics.
OutGroupMembResponses	Shows the outbound group member responses statistics.
OutGroupMembReductions	Shows the outbound group member reductions statistics.
OutRouterStatistics	Shows the outbound router statistics
OutRouterAdvertisements	Shows the outbound router advertisements statistics.
OutNeighborSolicits	Shows the outbound neighbor solicits statistics.
OutNeighborAdvertisements	Shows the outbound neighbor advertisements statistics.
OutMLDv2Reports	Shows the outbound MLDv2 reports statistics.
OutType133	Shows the outbound Type133 statistics.
OutType135	Shows the outbound Type135 statistics.
OutType143	Shows the outbound Type143 statistics.

View UDP Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view UDP statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IP/IPv6 UDP** tab.

IP/IPv6 UDP Field Descriptions

Use the data in the following table to use the IP/IPv6 UDP tab.

Name	Description
IPVersion	Shows the IP address version as ipv4 or ipv6.

Table continues…

Name	Description
InDatagrams	Shows the input datagram statistics.
NoPorts	Shows the number of ports statistics.
InErrors	Shows the input errors statistics.
OutDatagrams	Shows the output datagram statistics.
IgnoredMulti	Show the ignored multiport statistics.
RcvbufErrors	Shows the received buffer errors statistics.
SndbufErrors	Shows the send buffer errors statistics.
InCsumErrors	Shows the input checksum errors statistics.
Clear	Specifies to clear the statistics. Default is false.

View TCP Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view TCP statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IP/IPv6 TCP** tab.

IP/IPv6 TCP Field Descriptions

Use the data in the following table to use the IP/IPv6 TCP tab.

Name	Description
IPVersion	Shows the IP address version as ipv4 or ipv6.
ActiveOpens	Shows the active open TCP connections statistics.
PassiveOpens	Shows the passive open TCP connections statistics.
AttemptFails	Shows the TCP connection attempt failures statistics.
EstabResets	Shows the TCP connection esablished resets statistics.
InSegs	Shows the input segments statistics.
OutSegs	Shows the output segments statistics.
RetransSegs	Shows the retransmit segments statistics.
InErrs	Shows the input checksum errors statistics.
OutRsts	Shows the output resets statistics.

Table continues…

Name	Description
InCsumErrors	Shows the input checksum errors statistics.
Clear	Specifies to clear the statistics. Default is false.

View TCP Connections and UDP Endpoints Statistics for a Segmented Management Instance

Note:

This procedure does not apply to VSP 8600 Series.

Use this task to view TCP connections and UDP endpoints statistics for a Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select **Stats**.
4. Select the **IP/IPv6 Socket (TCP/UDP)** tab.

IP/IPv6 Socket (TCP/UDP) Field Descriptions

Use the data in the following table to use the IP/IPv6 Socket (TCP/UDP) tab.

Name	Description
IPVersion	Shows the IP address version as ipv4 or ipv6.
Type	Shows the connection type as tcp or udp.
Index	Shows the index ID for the connection.
State	Shows the link state for the connection.
RecvQ	Shows the connection received quanitity.
SendQ	Shows the connection sent quantity.
LocalAddressAndPort	Shows the local IP address and port.
PeerAddressAndPort	Shows the peer IP address and port.

Segmented Management Instance Configuration for VSP 8600 Series using EDM

Note:

This section only applies to VSP 8600 Series.

This section provides procedures to configure segmented management instance using the EDM.

Configure a Segmented Management Instance

Note:

This procedure only applies to VSP 8600 Series.

You must create a Management Instance to gain access to specific management applications.

About this task

The Management Instance supports different management interface types. When you create the Management Instance, you specify the interface type and the switch automatically creates the appropriate instance ID for that type.

In a Layer 3 routing or Fabric deployment, use a management CLIP.

Each Management Instance supports a single IPv4 and IPv6 (global scope) management address for use by management applications.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **MgmtInterface** tab.
4. Select **Insert**.
5. In the **InterfaceType** field, select the type of Management Instance to create.
6. **(Optional)** For a CLIP Management Instance, in the **VrfName** field, type the VRF name to associate with the CLIP instance.

   Note:

   If you want to associate the GRT with the CLIP instance, type **GlobalRouter** in the **VrfName** field. You cannot use mgmtrouter as the VRF.

   If you specify a non-default VRF, you must enable Layer 3 VSN to achieve IPv6 CLIP connectivity.
7. Select the **State** check box to enable the instance.
8. Select **Insert**.

MgmtInterface field descriptions

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

Name	Description
InstanceId	Shows a value that identifies the Management Instance type associated with this entry.
InterfaceType	Indicates the interface type.
VrfName	Specifies the VRF name to associate with the management CLIP .

Table continues…

Name	Description
State	Indicates if the interface is enabled for this instance. The default is disabled.
InterfaceMacAddr	Shows the MAC address for the interface.
InterfaceName	Shows the interface name.

Configure a Segmented Management Instance IP Address

✱ **Note:**

This procedure only applies to VSP 8600 Series.

After you create the Management Instance, you can add an IP address to it, and then configure route redistribution to advertise reachability of the Management Instance to the rest of the network.

Before you begin

- Ensure the IP address you plan to assign is not in use by an existing VLAN or CLIP IP subnet configured on the switch.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **MgmtAddress** tab.

   ✚ **Tip:**

   If you create the interface and assign an IP address during the same EDM session, you may need to select **Refresh** on the **MgmtAddress** tab before you see the new interface to configure.
4. To assign an IPv4 address:
   a. Select the **IpAddress** field, and then type the IPv4 address value.
   b. Select the **IpMask** field, and then type the IPv4 Mask value.
5. To assign an IPv6 address:
   a. Select the **Ipv6Address** field, and then type the IPv6 address value.
   b. Select the **Ipv6PrefixLength** field, and then type the IPv6 prefix value.
6. Select **Apply**.

MgmtAddress Field Descriptions

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

Name	Description
InstanceId	Shows a value that identifies the Management Instance type associated with this entry.

Table continues…

Name	Description
IpAddress	Specifies the IPv4 management address.
IpMask	Specifies the subnet mask of the IPv4 management address.
Ipv6Address	Specifies the IPv6 management address. Each Management Instance supports a single IPv6 management address for use by management applications.
Ipv6PrefixLength	Specifies the prefix length of the IPv6 management address. It is /128 for a loopback interface.
Ipv6LinkLocalAddr	Shows the automatically generated link local address.
InterfaceName	Shows the interface name.

View IPv4 Operational Routes for a Segmented Management Instance

✱ **Note:**

This procedure only applies to VSP 8600 Series.

Use this task to view IPv4 operational routes.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **MgmtIpRoute** tab.

MgmtIpRoute Field Descriptions

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

Name	Description
DestAddr	Shows the destination address of the route entry.
DestMask	Shows the destination mask of the route entry.
Metric	Shows the metric, or cost, assigned to the route entry. If multiple entries exist to the same destination, the metric determines which route is used. Routes with a type of LOCAL have a metric equal to 256.
Instance	Shows the Management Instance ID.
NextHop	Shows the next hop for the route entry.
IntfName	Shows the Management Instance interface name for the route entry.
Type	Shows the type of route entry.

View IPv6 Operational Routes for a Segmented Management Instance

Note:

This procedure only applies to VSP 8600 Series.

Use this task to view IPv6 operational routes.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **MgmtIpv6Route** tab.

MgmtIpv6Route Field Descriptions

Use the data in the following table to use the MgmtIpv6Route tab.

Name	Description
DestAddr	Shows the destination address of the route entry.
PrefixLen	Shows the destination prefix length of the route entry.
Metric	Shows the metric, or cost, assigned to the route entry. If multiple entries exist to the same destination, the metric determines which route is used. Routes with a type of LOCAL have a metric equal to 256.
Instance	Shows the Management Instance ID.
NextHop	Shows the next hop for the route entry.
IntfName	Shows the Management Instance interface name for the route entry.
Type	Shows the type of route entry.

Migrate an IP Address to a Segmented Management Instance

Note:

This procedure only applies to VSP 8600 Series.

Use this procedure to designate an existing VLAN or loopback IP address as a Segmented Management Instance. This action moves the IP interface from the VOSS routing stack to the management stack to use with management applications.

About this task

You cannot migrate interfaces used for routing purposes, for example, where you configure Layer 3 routing protocols.

This command does not apply to the OOB or mgmtEthernet interface. Releases that support this migration procedure automatically move the IP address on the mgmtEthernet interface from the routing stack to the Segmented Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **MgmtMigrate** tab.
4. Select **Insert**.
5. Select the instance type, either **clip** or **vlan**.
6. Specify the existing VLAN or loopback ID.
7. Select **Insert**.

MgmtMigrate field descriptions

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

Name	Description
InstanceId	Specifies the interface instance to migrate.
InterfaceIndex	Shows the interface index of the identified interface.
InterfaceType	Shows the interface type.
Description	Shows the interface description.
VlanId	Specifies the VLAN ID for a port-based VLAN.
LoopbackId	Specifies the loopback ID.
VrfName	Shows the VRF associated with the loopback interface.
IpAddress	Shows the IPv4 address to migrate.
IpMask	Shows the subnet mask for the IPv4 address.
Ipv6Address	Shows the IPv6 address to migrate.
Ipv6PrefixLength	Shows the prefix length for the IPv6 address.

View Segmented Management Instance Statistics

Note:

This procedure only applies to VSP 8600 Series.

View operational statistics for the Management Instance.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **Mgmt Instance**.
3. Select the **Mgmt Instance** tab.

4. Select a Management Instance by placing the cursor in a cell within the applicable row.
5. Select **Graph**.

Interface Counters Field Descriptions

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

Name	Description
RxPkts	Counts the packets received on the Segmented Management Instance.
RxError	Counts the packets received with errors on the Segmented Management Instance.
RxDrop	Counts the packets received and dropped on the Segmented Management Instance.
TxPkts	Counts the packets transmitted on the Segmented Management Instance.
TxError	Counts the packets transmitted with errors on the Segmented Management Instance.
TxDrop	Counts the packets dropped before transmission on the Segmented Management Instance.

Chapter 18: Bidirectional Forwarding Detection

Table 49: Bidirectional Forwarding Detection (BFD) product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
BFD (IPv4)	VSP 4450 Series	VOSS 8.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 8.1
	VSP 7400 Series	VOSS 8.1
	VSP 8200 Series	VOSS 8.1
	VSP 8400 Series	VOSS 8.1
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
BFD (IPv6)	VSP 4450 Series	VOSS 8.1 demonstration feature
	VSP 4900 Series	VOSS 8.1 demonstration feature
	VSP 7200 Series	VOSS 8.1 demonstration feature
	VSP 7400 Series	VOSS 8.1 demonstration feature
	VSP 8200 Series	VOSS 8.1 demonstration feature
	VSP 8400 Series	VOSS 8.1 demonstration feature
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
BFD over Fabric Extend Tunnels (IPv4)	VSP 4450 Series	Not Supported
	VSP 4900 Series	VOSS 8.2
	VSP 7200 Series	VOSS 8.2
	VSP 7400 Series	VOSS 8.2
	VSP 8200 Series	VOSS 8.2
	VSP 8400 Series	VOSS 8.2
	VSP 8600 Series	Not supported
	XA1400 Series	VOSS 8.2

Use Bidirectional Forwarding Detection (BFD) to provide a failure detection mechanism between two systems.

The following sections provide information and procedures for BFD.

BFD Fundamentals

The following sections provide fundamentals information about Bidirectional Forwarding Detection (BFD).

BFD Overview

Bidirectional Forwarding Detection (BFD) is a simple Hello protocol used between two peers. In BFD, peer systems periodically transmit BFD packets to each other. If one of the systems does not receive a BFD packet after a certain period of time, the system assumes that the link or other system is not operating.

A path is considered operational when bidirectional communication is established between systems. However, this does not preclude the use of unidirectional links.

BFD provides low-overhead, short-duration failure detection between two systems. BFD also provides a single mechanism for connectivity detection over any media, at any protocol layer.

Because BFD sends rapid failure-detection notifications to the routing protocols that run on the local system, which initiates routing table recalculations, BFD helps reduce network convergence time.

BFD supports IPv4/IPv6 single hop detection for static routes, OSPFv2, OSPFv3, iBGP, iBGPv6. Forwarding path failure detection for Fabric Extend tunnels is supported over an IPv4 network only.

Note:

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

Note:

iBGPv6 is not supported in VRF.

BFD Operation

VOSS uses one BFD session for all protocols with the same destination. For example, if a network runs OSPFv2 and BGP across the same link with the same peer, only one BFD session is established, and BFD shares session information with both routing protocols.

You can enable BFD over data paths with specified OSPFv2 and OSPFv3 neighbors, BGP neighbors, static routing next-hop addresses, and Fabric Extend tunnels.

VOSS supports BFD asynchronous mode, which sends BFD control packets between two systems to activate and maintain BFD neighbor sessions. To reach an agreement with its neighbor about how rapidly failure detection occurs, each system estimates how quickly it can send and receive BFD packets.

A session begins with the periodic, slow transmission of BFD control packets. When bidirectional communication is achieved, the BFD session comes up.

After the session is up, the transmission rate of Control packets can increase to achieve detection time requirements. If Control packets are not received within the calculated detection time, the session is declared down. After a session is down, Control packet transmission returns to the slow rate.

If a session is declared down, it cannot come back up until the remote end signals that it is down (three-way handshake). A session can be kept administratively down by configuring the state of AdminDown.

In asynchronous mode, detection time is equal to the value of DetectMult received from the remote system multiplied by the agreed transmit interval of the remote system (the greater of RequiredMinRxInterval and DesiredMinTxInterval.) DetectMult is approximately equal to the number of sequential packets that must be missed to declare a session down.

BFD States

A session normally proceeds through three states; two states are used to establish a session (Init and Up) and one state is used to tear down a session (Down). This allows a three-way handshake for both session establishment and session teardown, assuring that both systems are aware of all session state changes. There is a fourth state (AdminDown) that you can use to administratively put a session down indefinitely.

- Down state: Indicates the session is down or has just been created. The session will remain in Down state until the remote system sends a BFD control packet indicating anything other than Up state. If the control packet signals Down state, the session advances to Init state. If the control packet signals Init state, the session advances to Up state.
- Init state: In this state, the host system establishes communications with the remote system and sends a request to move the session to the Up state, but the remote system has not yet recognized the request. A session remains in Init state until it receives a BFD control packet signaling Init or Up state, or until the connectivity timer expires, indicating communication with the remote system is lost.
- Up state: Indicates the BFD session is established and connectivity is working. A session remains in Up state until connectivity fails or until the session is taken down administratively.
- AdminDown state: Indicates the BFD session is being held down administratively. This causes the remote system to enter Down state and remain there until the local system exits AdminDown state.

BFD Configuration

The following sections provide conceptual information about BFD configuration. For detailed procedural information about BFD configuration, see BFD Configuration using CLI on page 465 and BFD Configuration using EDM on page 480.

Enable BFD

To enable Bidirectional Forwarding Detection (BFD) between 2 peers:

- Configure BFD globally.
- Configure BFD on the required interfaces of both peer systems.
- Enable BFD on the required routing protocols.
- Specify the next-hop device with which the switch initiates the BFD session.

Delete a BFD Session

To delete a BFD session, disassociate all applications with the BFD session, then administratively bring down the BFD session.

Note:

To successfully delete a BFD session, you must execute the commands in the following order:

1. Disassociate all applications from the BFD session.
2. Disable BFD at the global level or interface level, which transitions the BFD session to AdminDown state.

If you change the above order of operations, the BFD session is not deleted.

BFD Considerations

The following considerations apply to Bidirectional Forwarding Detection (BFD):

- BFD is supported only in asynchronous mode. Demand mode and echo functionalities are not supported.
- You configure BFD parameters on a per session basis, not on a per next-hop basis.
- BFD creates multiple sessions even though a neighbor shares an IP address.
- The granularity of the fault detection interval in BFD is 100 ms, and the minimum multiplier is 2.

  The minimum value for the transmit interval or the receive interval is 100 ms. If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

  You can configure a total of 16 BFD sessions. Of the 16 possible BFD sessions, you can configure a maximum of 4 BFD sessions with the minimum value for transmit interval or receive interval. You can configure the remaining BFD sessions with a transmit interval or a receive interval that is greater than or equal to the 200 ms default value.

- BFD is not supported over RSMLT links. This applies to BFD sessions over IPv4 interfaces and IPv6 interfaces.
- Inter-tunnel routing with 6in4 tunnels is not supported. This means that incoming IPv6 packets over a tunnel cannot be forwarded over another tunnel configured on the same VOSS switch.
- BFD for Interior Border Gateway Protocol (iBGP) and BGPv6 in VRF is not supported.
- Session dampening is not supported for BFD.
- BFD for eBGPv6 in VRF is not supported.
- VOSS supports BFD multihop only at the eBGP application level. For other applications, VOSS does not support BFD multihop, as defined by RFC 5883. However, there is no requirement for source and destination IP addresses to be in the same subnet.
- BFD over IPv6 Fabric Extend (FE) tunnels is not supported.
- The minimum value for the transmit interval or the receive interval is 1 second with a fault detection time of 3 seconds for BFD over IPv4 FE tunnels.
- BFD does not support a static route flag.
- BFD is not supported on a Virtual Router Redundancy Protocol (VRRP) interface.
- High Availability for BFD is not supported.
- You can configure a total of 256 BFD and Virtual Link Aggregation Control Protocol (VLACP) sessions.
- BFD packets cannot be mirrored when BFD is configured on the switch.

BFD Configuration using CLI

Use the following procedures to configure Bidirectional Forwarding Detection (BFD) using CLI. BFD provides low-overhead, short-duration failure-detection between two systems.

Enable BFD Globally

Note:

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD globally.

Note:

Enabling BFD globally does not establish a BFD session. To establish a BFD session, you must also configure BFD at the interface level and at the application level.

Procedure

1. Enter BFD Router Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   router bfd
   ```

2. Enable BFD:

   ```
   router bfd enable
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#router bfd
Switch:1(router-bfd)#router bfd enable
```

Configure BFD on an IPv4 Interface

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to enable and to configure Bidirectional Forwarding Detection (BFD) on an IPv4 interface. All interface configuration is performed at the VLAN, GigabitEthernet, or Loopback level.

Note:

Enabling BFD on an interface does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the application level.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   followed by one of the following:

   - `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}`
   - `interface loopback <1-256>`

- `interface vlan <1-4059>`

  Note:

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

2. Enable BFD on an interface:

   ```
   ip bfd enable
   ```

3. **(Optional)** Configure the transmit interval:

   ```
   ip bfd interval <100-65335>
   ```

4. **(Optional)** Configure the minimum receive interval:

   ```
   ip bfd min-rx <100-65335>
   ```

5. **(Optional)** Configure the multiplier:

   ```
   ip bfd multiplier <1-20>
   ```

6. **(Optional)** In GigabitEthernet Interface Configuration mode, you can configure a value for port:

   ```
   ip bfd port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

7. **(Optional)** In VLAN Interface Configuration mode, you can configure a value for VLAN:

   ```
   ip bfd vlan <1-4094>
   ```

8. **(Optional)** In Loopback Interface Configuration mode, you can configure a value for loopback:

   ```
   ip bfd loopback <1-256>
   ```

Variable Definitions

The following table defines parameters for the **`ip bfd`** 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
enable	Enable BFD on a port, VLAN, or loopback.
interval <100-65335>	Specifies the transmit interval in milliseconds. The default is 200 ms. **Note:** For XA1400 Series, the default is 1000 ms.

Table continues…

Variable	Value
	Note: The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
min-rx <100-65535>	Specifies the receive interval in milliseconds. The default is 200 ms. **Note:** For XA1400 Series, the default is 1000 ms. **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
multiplier <1-20>	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout. The default is 3. **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.
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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
vlan <1-4094>	Specifies the VLAN ID in the range of 1 to 4094.
loopback <1-256>	Specifies the Loopback ID in the range of 1 to 256.

Configure BFD on an IPv6 Interface

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to enable and to configure BFD on an IPv6 interface. All interface configuration is performed at the VLAN or GigabitEthernet level.

Note:

Enabling BFD on an interface does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the application level.

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

2. Enable BFD on an interface:

   ```
   ipv6 bfd enable
   ```

3. **(Optional)** Configure the transmit interval:

   ```
   ipv6 bfd interval <100-65335>
   ```

4. **(Optional)** Configure the minimum receive interval:

   ```
   ipv6 bfd min-rx <100-65335>
   ```

5. **(Optional)** Configure the multiplier:

   ```
   ipv6 bfd multiplier <1-20>
   ```

6. **(Optional)** In GigabitEthernet Interface Configuration mode, you can configure a value for port:

   ```
   ipv6 bfd port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

7. **(Optional)** In VLAN Interface Configuration mode, you can configure a value for VLAN:

   ```
   ipv6 bfd vlan <1-4094>
   ```

Variable Definitions

The following table defines parameters for the **`ip bfd`** 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
enable	Enable BFD on a port, VLAN, or loopback.
interval <100-65335>	Specifies the transmit interval in milliseconds. The default is 200 ms.

Table continues…

Variable	Value
	Note: For XA1400 Series, the default is 1000 ms. **Note:** The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
min-rx <100-65535>	Specifies the receive interval in milliseconds. The default is 200 ms. **Note:** For XA1400 Series, the default is 1000 ms. **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
multiplier <1-20>	Specifies the multiplier used to calculate the amount of time BFD waits before declaring a receive timeout. The default is 3. **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.
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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
vlan <1-4094>	Specifies the VLAN ID in the range of 1 to 4094.
loopback <1-256>	Specifies the Loopback ID in the range of 1 to 256.

Enable BFD at the BGP Application Level

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD supports internal Border Gateway Protocol (iBGP) and external Border Gateway Protocol (eBGP) on IPv4 interfaces. You configure BFD on a VRF instance the same way you configure the GlobalRouter, except that you must use VRF Router Configuration mode and the prefix `ip bgp`. BFD does not support BGPv6 for VRF on IPv6 interfaces.

Note:

Enabling BFD at the BGP application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. Enter BGP Router Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   router bgp
   ```

2. Enable BFD for the BGP protocol:

   ```
   neighbor WORD<0-1536> fall-over bfd
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#router bgp
Switch:1(router-bgp)#neighbor 192.0.2.15 fall-over bfd
```

Variable Definitions

The following table defines parameters for the **`neighbor`** command.

Variable	Value
WORD<0-1536>	Specifies the peer IP address or the peer group name.

Enable BFD at the OSPF Application Level

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD supports Open Shortest Path First (OSPF) for IPv4 interfaces and OSPFv3 for IPv6 interfaces.

Use the following procedure to enable BFD at the OSPF application level.

Note:

Enabling BFD at the OSPF application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

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

2. **(Optional)** Enable BFD on an IPv4 interface under the OSPF protocol:

   ```
   ip ospf bfd
   ```

3. Enable BFD on an IPv6 interface under the OSPF protocol:

   ```
   ipv6 ospf bfd
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface gigabitethernet 1/3
Switch:1(config-if)#ip ospf bfd
```

Variable Definitions

The following table defines parameters for the **`ip ospf bfd`** command.

Table 50:

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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
<1-4059>	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. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Configure BFD on an IPv4 Static Route

Note:

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to configure BFD on an IPv4 static route.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure BFD on an IPv4 static route:

```
ip route bfd {A.B.C.D}
```

Variable Definitions

The following table defines parameters for the **ip route bfd** command.

Table 51:

Variable	Value
{A.B.C.D}	Specifies the BFD static route IPv4 address.

Configure BFD on an IPv6 Static Route

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to configure BFD on an IPv6 static route.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure BFD on an IPv6 static route:

```
ipv6 route bfd WORD<0-128>
```

3. **(Optional)** Configure an IPv6 static route for a port:

```
ipv6 route bfd WORD<0-128> port {slot/port[/sub-port] [-slot/port[/
sub-port]] [,...]}
```

4. **(Optional)** Configure an IPv6 static route for a VLAN:

```
ipv6 route bfd WORD<0-128> vlan <1-4094>
```

Variable Definitions

The following table defines parameters for the **ipv6 route bfd** command.

Variable	Value
WORD<0-128>	Specifies the BFD static route IPv6 address.
port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Specifies the port number for the BFD IPv6 static route.
vlan <1-4094>	Specifies the VLAN ID for the BFD IPv6 static route.

Clear BFD Session Statistics

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to clear local and remote Bidirectional Forwarding Detection (BFD) session statistics for IPv4 or IPv6 interfaces.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. **(Optional)** Clear BFD session statistics for an IPv4 interface:

   ```
   clear ip bfd stats
   ```

3. Clear BFD session statistics for an IPv6 interface:

   ```
   clear ipv6 bfd stats
   ```

Variable Definitions

The following table defines parameters for the **`clear ip bfd stats`** command.

Variable	Value
vrf WORD<1-16>	Specifies a VRF instance by VRF name.
vrfids WORD<0-512>	Specifies a VRF or range of VRFs by ID.

Display BFD Global Configuration

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use this procedure to display global configuration information for BFD.

Procedure

1. To enter User EXEC mode, log on to the switch.

2. Display global BFD configuration information:

   ```
   show ip bfd [vrf WORD<1-16>] [vrfids WORD<0-512>]
   ```

Example

The following example displays global configuration information for BFD on an IPv4 interface.

```
Switch:1>show ip bfd
================================================================================
                         BFD information - GlobalRouter
================================================================================
                      BFD Version :  1
                     Admin Status :  TRUE
                      Trap Enable :  FALSE
--------------------------------------------------------------------------------
   Total session number :  1

    UP: 1, DOWN: 0, AdminDown: 0, Init: 0
--------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for the **show ip bfd** command.

Table 52:

Variable	Value
vrf WORD<1-16>	Specifies a VRF instance by VRF name.
vrfids WORD<0-512>	Specifies a VRF or range of VRFs by ID.

Display BFD Configuration at the Interface Level

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to display BFD configuration on an interface.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display BFD on a Gigabit Ethernet interface:

   ```
   show ip bfd interfaces Gigabitethernet [{slot/port[/sub-port][-slot/
   port[/sub-port]][,...]}] [vrf WORD<1-16>] [vrfids WORD<0-512>]
   ```

3. Display BFD on a VLAN interface:

   ```
   show ip bfd interfaces vlan [<1-4059>] [vrf WORD<1-16>] [vrfids
   WORD<0-512>]
   ```

Example

The following example displays VLAN interface configuration information for BFD.

```
Switch:1>show ip bfd interfaces vlan 11
==========================================================================================
                                    Vlan Bfd
==========================================================================================
VLAN       STATUS     MIN_RX     INTERVAL   MULTIPLIER      VRF-ID
------------------------------------------------------------------------------------------
11         enable     200        200        3               0
```

The following example displays Loopback interface configuration information for BFD:

```

Switch:1>enable
Switch:1#show ip bfd interfaces loopback
================================================================================
                          Circuitless IP Interface Bfd
================================================================================
INTF ID    STATUS     MIN_RX     INTERVAL   MULTIPLIER      VRF-ID
--------------------------------------------------------------------------------
1          enable     200        200        3               0
2          enable     200        200        3               2
```

Variable Definitions

The following table defines parameters for the **show ip bfd interfaces** 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
<1-4059>	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. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
vrf WORD<1-16>	Specifies a VRF instance by VRF name.
vrfids WORD<0-512>	Specifies a VRF or range of VRFs by ID.

Display BFD Configuration for an IPv6 Interface

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to display BFD configuration on an IPv6 interface.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display BFD on a Gigabit Ethernet interface:

   `show ipv6 bfd interfaces Gigabitethernet [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]`

3. Display BFD on a VLAN interface:

   `show ipv6 bfd interfaces vlan <1-4059>`

Example

The following example displays port configuration information for BFD.

```
Switch:1>show ipv6 bfd interfaces gigabitethernet 1/3

==========================================================================================
                                    Port Bfd
==========================================================================================
PORT       STATUS     MIN_RX     INTERVAL   MULTIPLIER      VRF-ID
------------------------------------------------------------------------------------------
1/3        enable     200        200            3           0
```

Variable Definitions

The following table defines parameters for the **`show ip bfd interfaces`** 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 the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
<1-4059>	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. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
vrf WORD<1-16>	Specifies a VRF instance by VRF name.
vrfids WORD<0-512>	Specifies a VRF or range of VRFs by ID.

Display BFD Neighbor Information

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use this procedure to display BFD session information for IPv4 neighbors.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display BFD neighbor information:

   `show ip bfd neighbors`
3. **(Optional)** Display BFD neighbor next-hop information:

   `show ip bfd neighbors next-hop {A.B.C.D}`
4. **(Optional)** Display BFD neighbor information for a particular VRF:

   `show ip bfd neighbors vrf WORD<1-16>`
5. **(Optional)** Display BFD neighbor information for a VRF ID or a range of VRF IDs:

   `show ip bfd neighbors vrfids WORD<0-512>`

Example

The following example displays BFD session information for an IPv4 neighbor.

```
Switch:1>show ip bfd neighbors
========================================================================================================================
                                          BFD Session - GlobalRouter
========================================================================================================================

MY_DISC    YOUR_DISC  NEXT_HOP        STATE      MULTI MIN_TX MIN_RX ACT_TX DETECT_TIME REMOTE_STATE APP    RUN

1          0          192.0.2.11      Down       3     200    200    1000   600         Down         O
------------------------------------------------------------------------------------------------------------------------
  1 out of 1 BFD session displayed
------------------------------------------------------------------------------------------------------------------------
APP and RUN Legend:
        B=BGP, O=OSPF, S=Static Route
------------------------------------------------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for the **`show ip bfd neighbors`** command.

Variable	Value
{A.B.C.D}	Specifies the next-hop IP address in the format a.b.c.d.
vrf WORD<1-16>	Specifies a VRF instance by name (the string length ranges from 1–16 characters).
vrfids WORD<0-512>	Specifies a range of VRFs by ID number (the ID ranges from 0–512).

Display BFD IPv6 Neighbor Information

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use this procedure to display information about BFD IPv6 neighbors.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display BFD neighbor information:

   `show ipv6 bfd neighbors`
3. **(Optional)** Display BFD neighbor next-hop information:

   `show ipv6 bfd neighbors next-hop WORD<0-128>`
4. **(Optional)** Display BFD neighbor information for a particular VRF:

   `show ipv6 bfd neighbors vrf WORD<1-16>`
5. **(Optional)** Display BFD neighbor information for a range of VRFs:

   `show ipv6 bfd neighbors vrfids WORD<0-512>`

Example

The following example displays BFD session information for an IPv6 neighbor.

```
Switch:1>show ipv6 bfd neighbors
=========================================================================================================================================
                                          BFD Session - GlobalRouter
=========================================================================================================================================

MY_DISC    YOUR_DISC  NEXT_HOP                            STATE      MULTI MIN_TX MIN_RX ACT_TX DETECT_TIME REMOTE_STATE APP    RUN
1          0          2001:DB8:0:0:25AB:0:0:1             Down       3     200    200    1000   0           Down         O
-----------------------------------------------------------------------------------------------------------------------------------------
  1 out of 1 BFD session displayed
-----------------------------------------------------------------------------------------------------------------------------------------
APP and RUN Legend:
        B=BGP_IPv6, O=OSPFv3, S=IPv6 Static Route
-----------------------------------------------------------------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for the **`show ipv6 bfd neighbors`** command.

Variable	Value
WORD<0-128>	Specifies the next-hop IPv6 address in the format a:b:c:d:e:f:g:h.
vrf WORD<1-16>	Specifies a VRF instance by name (the string length ranges from 1–16 characters).
vrfids WORD<0-512>	Specifies a range of VRFs by ID number (the ID ranges from 0–512).

Display BFD Statistics

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

Use the following procedure to display BFD statistics for IPv4 or IPv6 interfaces.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display BFD IPv4 statistics:

```
show ip bfd stats [vrf] [vrfids]
```

3. Display BFD IPv6 statistics:

```
show ipv6 bfd stats [vrf] [vrfids]
```

Example

The following example displays BFD statistics for IPv4 interfaces.

```
Switch:1>show ip bfd stats
==========================================================================================
                              BFD staticstics - GlobalRouter
==========================================================================================

MY_DISC    YOUR_DISC  NEXT_HOP     PACKT_IN     PACKET_OUT   LAST_UP    LAST_DOWN
------------------------------------------------------------------------------------------

1          0          192.0.2.10   4661750      4620630      16007202   84431796
------------------------------------------------------------------------------------------
```

The following example displays BFD statistics for IPv6 interfaces.

```
Switch:1>show ipv6 bfd stats
==========================================================================================
                              BFD staticstics - GlobalRouter
==========================================================================================

MY_DISC YOUR_DISC NEXT_HOP                PACKT_IN     PACKET_OUT   LAST_UP    LAST_DOWN
------------------------------------------------------------------------------------------

1       0        2001:DB8:0:0:0:0:0:ffff  4661750      4620630      16007202   84431796
------------------------------------------------------------------------------------------
```

Variable Definitions

The following table defines parameters for the **`show ip bfd stats`** command.

Variable	Value
vrf	Specifies a VRF instance by VRF name.
vrfids	Specifies a VRF or range of VRFs by ID.

BFD Configuration using EDM

Use the following procedures to configure Bidirectional Forwarding Detection (BFD) using EDM. BFD provides low-overhead, short-duration failure-detection between two systems.

Enable BFD Globally

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD globally.

Note:
Enabling BFD globally does not establish a BFD session. To establish a BFD session, you must enable BFD at the interface level and at the application level.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **BFD**.
3. Select the **Globals** tab.
4. In the **AdminStatus** field, select **enabled**.
5. **(Optional)** Select **TrapEnabled** to send BFD traps.

BFD Globals Field Descriptions

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

Name	Description
AdminStatus	Specifies whether BFD is enabled.
VersionNumber	Specifies the current version number of the BFD protocol.
TrapEnabled	Specifies whether BFD traps are sent.

Display BFD Sessions

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to display information about BFD sessions. You can optionally display BFD session information for IPv4 or IPv6 interfaces.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **BFD**.
3. Select the **Sessions** tab.
4. **(Optional)** Select **Filter**.
5. **(Optional)** Select **AddrType**.
6. **(Optional)** In the **AddrType** field, specify a value for address type.

BFD Sessions Field Descriptions

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

Name	Description
Discriminator	Specifies the local discriminator that uniquely identifies the BFD session.
RemoteDiscr	Specifies the discriminator of the remote system in the BFD session.
UdpPort	Specifies the UDP Port for the BFD session. The default value is the well-known value for the port.
State	Specifies the state of the BFD session. Possible values are Down, Up, Init, and AdminDown.
Addr	Specifies the IP address of the interface associated with the BFD session. A value of unknown (0) indicates the BFD session is not associated with a specific interface.
DesiredMinTxInterval	Specifies the preferred minimum interval for transmitting BFD control packets by the local system.
ReqMinTxInterval	Specifies he minimum interval for transmitting BFD control packets that the local system can support.
DestAddr	Specifies the destination IP address of the interface associated with the BFD session.
OldState	Specifies the old state of the BFD session.
App	Specifies the applications configured on the BFD session.
AppRun	Specifies the applications running on the BFD session.
AddrType	Specifies the IP address type of the interface associated with this BFD session. Possible values are ipv4 and ipv6.

Configure BFD for an IPv4 Interface on a Port

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable and configure BFD for an IPv4 interface on a port.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Port**.
2. Select **IP**.

3. Select the **BFD** tab.
4. Select **Enable**.
5. **(Optional)** In the **MinRxInterval** field, specify the minimum receive interval..
6. **(Optional)** In the **TxInterval** field, specify the transmit interval.
7. **(Optional)** In the **Multiplier** field, specify a value for the multiplier used to calculate a receive timeout.

BFD Field Descriptions

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

Name	Description
Enable	Enable BFD on the port.
MinRxInterval	Specifies the minimum interval, in milliseconds, between received BFD control packets that the local system is capable of supporting. The default is 200 ms. **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
TxInterval	Specifies the transmit interval in milliseconds. The default is 200 ms. **Note:** The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
Multiplier	Specifies a value for the multiplier used to calculate a receive timeout. The default is 3. **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

Configure BFD for an IPv6 Interface on a Port

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable and configure BFD for an IPv6 interface on a port.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit** > **Port**.
2. Select **IPv6**.
3. Select the **IPv6 BFD Interface** tab.
4. **(Optional)** In the **MinRxInterval** column, double-click the field and type a value for **MinRxInterval**.
5. **(Optional)** In the **TxInterval** column, double-click the field and type a value for **TxInterval**.
6. **(Optional)** In the **Multiplier** column, double-click the field and type a value for **Multiplier**.

BFD Field Descriptions

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

Name	Description
Interface	Specifies the BFD interface.
MinRxInterval	Specifies the minimum interval, in milliseconds, between received BFD control packets that the local system is capable of supporting. The default is 200 ms. **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
TxInterval	Specifies the transmit interval in milliseconds. The default is 200 ms.

Table continues…

Name	Description
	Note: The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
Multiplier	Specifies a value for the multiplier used to calculate a receive timeout. The default is 3. **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

Configure BFD for an IPv4 Interface on a VLAN

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure detection-mechanism between two systems. Use the following procedure to enable and configure BFD for an IPv4 interface on a VLAN.

Procedure

1. In the navigation pane, expand **Configuration** > **VLAN**.
2. Select **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN on which you want to configure BFD.
5. Select **IP**.
6. Select **BFD**.
7. Select **Enable**.
8. **(Optional)** In the **MinRxInterval** field, specify the minimum receive interval..
9. **(Optional)** In the **TxInterval** field, specify the transmit interval.
10. **(Optional)** In the **Multiplier** field, specify a value for the multiplier used to calculate a receive timeout.

IP BFD field descriptions

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

Name	Description
Enable	Enable BFD on the VLAN.
MinRxInterval	Specifies the minimum interval, in milliseconds, between received BFD control packets that the local system is capable of supporting. The default is 200 ms. ✱ **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
TxInterval	Specifies the transmit interval in milliseconds. The default is 200 ms. ✱ **Note:** The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
Multiplier	Specifies a value for the multiplier used to calculate a receive timeout. The default is 3. ✱ **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

Configure BFD for an IPv6 Interface on a VLAN

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable and configure BFD for an IPv6 interface on a VLAN.

Procedure

1. In the navigation pane, expand **Configuration** > **VLAN**.
2. Select **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN on which you want to configure BFD.
5. Select **IPV6**.
6. Select **IPv6 BFD Interface**.
7. **(Optional)** In the **MinRxInterval** column, double-click the field and type a value for **MinRxInterval**.
8. **(Optional)** In the **TxInterval** column, double-click the field and type a value for **TxInterval**.
9. **(Optional)** In the **Multiplier** column, double-click the field and type a value for **Multiplier**.

IPV6 BFD Interface field descriptions

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

Name	Description
Interface	Specifies an index value that uniquely identifies the interface.
Enable	Enable BFD on the VLAN.
MinRxInterval	Specifies the minimum interval, in milliseconds, between received BFD control packets that the local system is capable of supporting. The default is 200 ms. **Note:** The minimum value you can configure for the receive interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the receive interval. You can configure any remaining BFD sessions with a receive interval that is greater than or equal to the 200 ms default value.
TxInterval	Specifies the transmit interval in milliseconds. The default is 200 ms. **Note:** The minimum value you can configure for the transmit interval is 100 ms. You can configure a maximum of 4 BFD sessions with the minimum value for the transmit interval. You can

Table continues…

Name	Description
	configure any remaining BFD sessions with a transmit interval that is greater than or equal to the 200 ms default value.
Multiplier	Specifies a value for the multiplier used to calculate a receive timeout. The default is 3. ✱ **Note:** If you configure the transmit interval or the receive interval as 100 ms, you must configure a value of 4 or greater for the multiplier.

Enable BFD for BGP Peers

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD for Border Gateway Protocol (BGP) peers.

✱ **Note:**
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the navigation pane, expand **Configuration** > **IP**.
2. Select **BGP**.
3. Select the **Peers** tab.
4. Select **Insert**.
5. Select **BfdEnable**.

Peers Field Descriptions

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

Name	Description
Instance	Specifies the BGP peer instance.
LocalAddrType	Specifies the local IP address type of the entered BGP peer.
LocalAddr	Specifies the local IP address of the entered BGP peer.
RemoteAddrType	Specifies the remote IP address type of the entered BGP peer.
RemoteAddr	Specifies the remote IP address of the entered BGP peer.
AdminStatus	Specifies the administrative status of the BGP peer.
GroupName	Specifies the peer group name to which the peer belongs (optional).

Table continues…

Name	Description
PeerState	Specifies the BGP peer connection state.
RemoteAs	Configures a remote AS number for the peer or peer-group in the range 0–65535.
Enable	Controls whether the peer connection is enabled or disabled. The default is disabled.
EbgpMultiHop	Enables or disables a connection to a BGP peer that is more than one hop away from the local router. The default value is disable.
RoutePolicyIn	Specifies the policy (by name) that applies to all network routes learned from this peer.
RoutePolicyOut	Specifies the policy (by name) that applies to all outgoing route updates.
RemovePrivateAs	Strips (when enabled) private AS numbers when the switch sends an update. The default is enable.
UpdateSourceInterface	Specifies the source IP address to use when the switch sends eBGP packets to this peer or peer group.
ConnectRetryInterval	Specifies the time interval, in seconds, for the connect retry timer. The suggested value for this timer is 120 seconds. The range is 1 to 65535.
HoldTimeConfigured	Specifies the time interval, in seconds, for the hold time for this BGP speaker with this peer. This value is in an open message sent to this peer by this BGP speaker. To determine the hold time with the peer, the switch compares this value with the HoldTime value in an open message received from the peer. The HoldTime must be at least three seconds. If the value is zero, the hold time does not establish with the peer. The suggested value for this timer is 180 seconds. The range is 0 to 65535.
KeepAliveConfigured	Specifies the time interval, in seconds, for the KeepAlive timer configured for this BGP speaker with this peer. KeepAliveConfigured determines the keep alive message frequency relative to HoldTimeConfigured; KeepAlive indicates the actual time interval for the keep alive messages. The recommended maximum value for this timer is one-third of HoldTimeConfigured. If KeepAliveConfigured is zero, no periodic keep alive messages are sent to the peer after the peers establish a BGP connection. Configure a value of 60 seconds. The range is 0 to 21845.
MD5Authentication	Enables and disables MD5 authentication.
AdvertisementInterval	Specifies the time interval, in seconds, that elapses between each transmission of an advertisement from a BGP neighbor. The default value is 30 seconds and the range is 5–120 seconds. The route advertisement interval feature is implemented using the time stamp that indicates when each route is advertised. The time stamp is marked to each route so that the route advertisement interval is compared to the time stamp and BGP is then able to make

Table continues…

Name	Description
	a decision about whether the route advertisement can be sent or should be delayed when a better route is received. This feature does not work for a withdraw route because the route entry is already removed when the processing route advertisement is sent and the time stamp marked in the route entry cannot be obtained.
DefaultOriginate	When enabled, specifies that the current route originated from the BGP peer. This parameter enables or disables sending the default route information to the specified neighbor or peer. The default value is false.
DefaultOriginateIpv6	When enabled, specifies that the current IPv6 route originated from the BGP peer. This parameter enables or disables sending the default IPv6 route information to the specified neighbor or peer. The default value is false.
Weight	Specifies the peer or peer group weight, or the priority of updates the system can receive from this BGP peer. The default value is 100 and the range is 0–65535.
MaxPrefix	Configures a limit on the number of routes accepted from a neighbor. The default value is 12000 routes and the range is 0–2147483647. A value of 0 means no limit exists.
NextHopSelf	Specifies that the next-hop attribute in an iBGP update is the address of the local router or the router that generates the iBGP update. The default is disable.
RouteReflectorClient	Specifies that this peer is a route reflector client. **Note:** This parameter only applies to VRF 0.
SoftReconfigurationIn	When enabled, the router relearns routes from the specified neighbor or group of neighbors without restarting the connection after the policy changes in the inbound direction. The default value is disable. Enabling SoftReconfigurationIn stores all BGP routes in local memory (even non-best routes).
DebugMask	Displays the specified debug information for the BGP peer. The default value is none. • None disables all debug messages. • Event enables the display of debug event messages. • State enables display of debug state transition messages. • Update enables display of debug messages related to updates transmission and reception. • Error enables the display of debug error messages. • Trace enables the display of debug trace messages.

Table continues…

Name	Description
	• Init enables the display of debug initialization messages. • All enables all debug messages. • Packet enables the display of debug packet messages. • Warning enables the display of debug warning messages. • Filter enables the display of debug messages related to filtering.
SendCommunity	Enables or disables sending the community attribute of the update message to the specified peer. The default value is disable.
Vpnv4Address	Specifies the vpnv4 routes.
IpvpnLiteCap	Enable or disable IP VPN-lite capabilitiy on the BGP neighbor peer.
Ipv6Cap	Enable or disable the IPv6 capability on the BGP neighbor peer. The default value is disable.
SooAddress	Specifies the site-of-origin (SoO) address of the BGP peer.
SooAsNumber	Specifies the site-of-origin (SoO) Autonomous System (AS) number of the BGP peer.
SooAssignedNum	Specifies the site-of-origin (SoO) assigned number of the BGP peer.
SooType	Specifies the site-of-origin (SoO) type of the BGP peer.
RouteRefresh	Enables or disables route refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates in the database that are eligible for the peer that issues the request. This parameter only applies to VRF 0.
AsOverride **Note:** This field does not appear on all hardware platforms.	Specifies that the AS Override parameter can be enabled or disabled for the BGP peer. The default is disable.
AllowAsIn **Note:** This field does not appear on all hardware platforms.	Specifies the number of AS-in allowed for the BGP peer. The range is 1–10.
Ipv6RoutePolicyIn	Specifies the policy (by name) that applies to all network IPv6 routes learned from this peer.
Ipv6RoutePolicyOut	Specifies the policy (by name) that applies to all outgoing IPv6 route updates.
Ipv6MaxPrefix	Configures a limit on the number of IPv6 routes accepted from a neighbor. A value of 0 means no limit exists.
BfdEnable	Enables Bidirectional Forwarding Detection (BFD) for this BGP peer.

Enable BFD for BGP Peer Groups

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD for Border Gateway Protocol (BGP) peer groups.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the navigation pane, expand **Configuration** > **IP**.
2. Select **BGP**.
3. Select the **Peer Groups** tab.
4. Select **Insert**.
5. Select **BfdEnable**.

Peer Groups field descriptions

Use the data in the following table to use the **Peer Groups** tab.

Name	Description
Index	Specifies the index of this peer group.
GroupName	Specifies the peer group to which this neighbor belongs (optional).
Enable	Enables or disables the peer group.
RemoteAs	Configures a remote AS number for the peer-group in the range 0–65535.
DefaultOriginate	When enabled, the BGP speaker (the local router) sends the default route 0.0.0.0 to a group of neighbors for use as a default route. The default is disabled.
DefaultOriginateIpv6	When enabled, the BGP speaker (the local router) sends the default route to a group of neighbors for use as a default route. The default is disabled.
EbgpMultiHop	When enabled, the switch accepts and attempts BGP connections to external peers that reside on networks that do not directly connect. The default is disabled.
AdvertisementInterval	Specifies the time interval, in seconds, that elapses between BGP routing updates. The default value is 30 seconds.

Table continues…

Name	Description
KeepAlive	Specifies the time interval, in seconds, between sent BGP keep alive messages to remote peers. The default value is 60.
HoldTime	Configures the hold time for the group of peers in seconds. Use a value that is three times the value of the KeepAlive time. The default value is 180.
Weight	Assigns an absolute weight to a BGP network. The default value is 100.
MaxPrefix	Limits the number of routes accepted from this group of neighbors. A value of zero indicates no limit The default value is 12,000 routes.
NextHopSelf	Specifies that the switch must set the NextHop attribute to the local router address before it sends updates to remote peers.
RoutePolicyIn	Specifies the route policy that applies to all networks learned from this group of peers.
RoutePolicyOut	Specifies the route policy that applies to all outgoing updates to this group of peers.
RouteReflectorClient	Specifies that this peer group is a route reflector client. **Note:** This parameter only applies to VRF 0.
SoftReconfigurationIn	When enabled, the router relearns routes from the specified neighbor or group of neighbors without restarting the connection after the policy changes in the inbound direction. The default value is enable. Enabling SoftReconfigurationIn stores all BGP routes in local memory (even non-best routes).
MD5Authentication	Enables and disables MD5 authentication. The default is disable.
RemovePrivateAs	Strips (when enabled) private AS numbers when the switch sends an update. The default is enable.
SendCommunity	Enables or disables sending the community attribute of the update message to the specified peer group. The default value is disable.
AfUpdateSourceInterfaceType	Specifies the interface type.
AfUpdateSourceInterface	Specifies the IP address used for circuitless IP (CLIP) for this peer group.
Vpnv4Address	Enables BGP address families for IPv4 (BGP) and L3 VPN (MP-BGP) support. Enable this parameter for VPN/VRF Lite routes.
IpvpnLiteCap	Specifies (when enabled) that IP VPN Lite capability can be enabled or disabled on the BGP neighbor peer. The default is disable.
RouteRefresh	Enables or disables route refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request. This parameter only applies to VRF 0.

Table continues…

Name	Description
AsOverride	Specifies that the AS Override parameter can be enabled or disabled for the BGP peer group. The default is disable.
AllowedAsIn	Specifies the number of AS-in allowed for the BGP peer group. The range is 1–10.
IPv6Cap	Enable or disable the IPv6 capability on the BGP neighbor peer. The default value is disable.
Ipv6RoutePolicyIn	Specifies the policy (by name) that applies to all network IPv6 routes learned from this peer.
Ipv6RoutePolicyOut	Specifies the policy (by name) that applies to all outgoing IPv6 route updates.
Ipv6MaxPrefix	Configures a limit on the number of IPv6 routes accepted from a neighbor. A value of 0 means no limit exists.
BfdEnable	Enables Bidirectional Forwarding Detection (BFD) for the BGP peer group.

Enable BFD for BGPv6 Peers

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD for BGPv6 peers.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Note:

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

Procedure

1. In the navigation pane, expand **Configuration** > **IPv6**.
2. Select **BGP+**.
3. Select the **Peers** tab.
4. Select **Insert**.
5. Select **BfdEnable**.

Peers Field Descriptions

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

Name	Description
RemoteAddr	Specifies the remote IPv6 address of the entered BGP+ peer.
GroupName	Specifies the peer group name to which the peer belongs (optional).
PeerState	Specifies the BGPv6 peer connection state.
RemoteAs	Configures a remote AS number for the peer or peer-group in the range 0 to 65535.
Enable	Controls whether the peer connection is enabled or disabled. The default is disabled.
EbgpMultiHop	Enables or disables a connection to a BGPv6 peer that is more than one hop away from the local router. The default value is disable.
RoutePolicyIn	Specifies the policy (by name) that applies to all network routes learned from this peer.
RoutePolicyOut	Specifies the policy (by name) that applies to all outgoing route updates.
RemovePrivateAs	Strips (when enabled) private AS numbers when the switch sends an update. The default is enable.
UpdateSourceInterface	Specifies the source IP address to use when the switch sends eBGP packets to this peer or peer group.
ConnectRetryInterval	Specifies the time interval, in seconds, for the connect retry timer. The suggested value for this timer is 120 seconds. The range is 1 to 65535.
HoldTimeConfigured	Specifies the time interval, in seconds, for the hold time for this BGP speaker with this peer. This value is in an open message sent to this peer by this BGP speaker. To determine the hold time with the peer, the switch compares this value with the HoldTime value in an open message received from the peer. The HoldTime must be at least three seconds. If the value is zero, the hold time does not establish with the peer. The suggested value for this timer is 180 seconds. The range is 0 to 65535.
KeepAliveConfigured	Specifies the time interval, in seconds, for the KeepAlive timer configured for this BGP speaker with this peer. KeepAliveConfigured determines the keep alive message frequency relative to HoldTimeConfigured; KeepAlive indicates the actual time interval for the keep alive messages. The recommended maximum value for this timer is one-third of HoldTimeConfigured. If KeepAliveConfigured is zero, no periodic keep alive messages are sent to the peer after the peers establish a BGP connection. Configure a value of 60 seconds. The range is 0 to 21845.
MD5Authentication	Enables and disables MD5 authentication.
AdvertisementInterval	Specifies the time interval, in seconds, that elapses between each transmission of an advertisement from a BGPv6 neighbor. The default value is 30 seconds and the range is 5 to 120 seconds.

Table continues…

Name	Description
	The route advertisement interval feature is implemented using the time stamp that indicates when each route is advertised. The time stamp is marked to each route so that the route advertisement interval is compared to the time stamp and BGP is then able to make a decision about whether the route advertisement can be sent or it should be delayed when a better route is received. This feature does not work for a withdraw route because the route entry is already removed when the processing route advertisement is sent and the time stamp marked in the route entry cannot be obtained.
DefaultOriginateIpv6	When enabled, specifies that the current IPv6 route originated from the BGP peer. This parameter enables or disables sending the default IPv6 route information to the specified neighbor or peer. The default value is false.
Weight	Specifies the peer or peer group weight, or the priority of updates the system can receive from this BGP peer. The default value is 100 and the range is 0 to 65535.
MaxPrefix	Configures a limit on the number of routes accepted from a neighbor. The default value is 12000 routes and the range is 0 to 2147483647. A value of 0 means no limit exists.
NextHopSelf	Specifies that the next-hop attribute in an iBGP update is the address of the local router or the router that generates the iBGP update. The default is disable.
RouteReflectorClient	Specifies that this peer is a route reflector client. **Note:** This parameter only applies to VRF 0.
SoftReconfigurationIn	When enabled, the router relearns routes from the specified neighbor or group of neighbors without restarting the connection after the policy changes in the inbound direction. The default value is disable. Enabling SoftReconfigurationIn stores all BGP routes in local memory (even non-best routes).
DebugMask	Displays the specified debug information for the BGP peer. The default value is none. • None disables all debug messages. • Event enables the display of debug event messages. • State enables display of debug state transition messages. • Update enables display of debug messages related to updates transmission and reception. • Error enables the display of debug error messages. • Trace enables the display of debug trace messages. • Init enables the display of debug initialization messages.

Table continues…

Name	Description
	• All enables all debug messages. • Packet enables the display of debug packet messages. • Warning enables the display of debug warning messages. • Filter enables the display of debug messages related to filtering.
SendCommunity	Enables or disables sending the community attribute of the update message to the specified peer. The default value is disable.
IpvpnLiteCap	Enable or disable IP VPN-lite capabilitiy on the BGP neighbor peer.
Ipv6Cap	Enable or disable the IPv6 capability on the BGP neighbor peer. The default value is disable.
RouteRefresh	Enables or disables route refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request. This parameter only applies to VRF 0.
AsOverride **Note:** This field does not appear on all hardware platforms.	Specifies that the AS Override parameter can be enabled or disabled for the BGP peer. The default is disable.
AllowAsIn **Note:** This field does not appear on all hardware platforms.	Specifies the number of AS-in allowed for the BGP peer. The range is 1–10.
Ipv6RoutePolicyIn	Specifies the policy (by name) that applies to all network IPv6 routes learned from this peer.
Ipv6RoutePolicyOut	Specifies the policy (by name) that applies to all outgoing IPv6 route updates.
Ipv6MaxPrefix	Configures a limit on the number of IPv6 routes accepted from a neighbor. A value of 0 means no limit exists.
BfdEnable	Enables Bidirectional Forwarding Detection (BFD) for this peer.

Enable BFD for OSPF on an IPv4 Port Interface

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD for the OSPF protocol on an IPv4 port interface.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation pane, expand **Configuration** > **Edit** > **Port**.
3. Select **IP**.
4. Select the **OSPF** tab.
5. Select **BfdEnable**.

OSPF Field Descriptions

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

Name	Description
Enable	Enables or disables OSPF routing on the specified port. The default is false.
HelloInterval	Specifies the length of time, in seconds, between the transmission of hello packets. This value must be the same for all routers attached to a common network. The default is 10 seconds. After you change the hello interval values, you must save the configuration file, and then restart the switch. After the switch restarts, it restores the values and checks for consistency.
RtrDeadInterval	Specifies the interval used by adjacent routers to determine if the router was removed from the network. This interval must be identical on all routers on the subnet, and a minimum of four times the hello interval. To avoid interoperability issues, the RtrDeadInterval value for the OSPF interface needs to match with the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds.
DesigRtrPriority	Specifies the priority of this port in multiaccess networks to use in the designated router election algorithm. The value 0 indicates the router is not eligible to become the designated router on this particular network. If a tie occurs, routers use their router ID as a tie breaker. The default is 1.
Metric	Specifies the metric for the type of service (TOS) on this port. The value of the TOS metric is (10^9 / interface speed). The default is 1. • FFFF—No route exists for this TOS. • IPCP links—Defaults to 0. • 0—Use the interface speed as the metric value when the state of the interface is up.
AuthType	Specifies the type of authentication required for the interface. • none—Specifies that no authentication required. • simple password—Specifies that all OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey parameter.

Table continues…

Name	Description
	• MD5 authentication—Specifies that all OSPF updates received by the interface must contain the MD5 key. • sha1—Specifies secure hash algorithm (SHA-1), which is a cryptographic hash function that produces a 160-bit hash value, usually given in a hexadecimal number, 40 digits long. You can only access and enable the SHA-1 authentication type after you enable enhanced secure mode. • sha-2—Specifies SHA-2, which offers the hash function SHA-256. **Note:** sha-2, an update of SHA-1, can offer six hash functions that include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA 512/256, with hash values that are 224, 256, 384, or 512 bits. However, the current release supports only SHA-256.
AuthKey	Specifies the key (up to 8 characters) when you specify simple password authentication in the port AuthType variable.
AreaId	Specifies the OSPF area name in dotted-decimal format. The area name is not related to an IP address. You can use a suitable value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
AdvertiseWhenDown	Advertises the network on this port as up, even if the port is down. The default is false. After you configure a port with no link and enable AdvertiseWhenDown, it does not advertise the route until the port is active. Then, OSPF advertises the route even if the link is down. To disable advertising based on link-states, disable AdvertiseWhenDown.
IfType	Specifies the type of OSPF interface (broadcast, NBMA, or passive). Before you change an OSPF interface type, you must first disable the interface. If the interface is an NBMA interface, you must also delete all configured neighbors.
PollInterval	Specifies the length of time, in seconds, between hello packets sent to an inactive OSPF router. Neighbors must have the same poll interval.
IfMtuIgnore	Specifies whether the interface ignores the global maximum transmission unit (MTU) configuration. To allow the switch to accept OSPF database description (DD) packets with a different MTU size, enable MtuIgnore. The interface drops incoming OSPF DD packets if their MTU is greater than 1500 bytes.
BfdEnable	Enable Bidirectional Forwarding Detection (BFD) for OSPF.

Enable BFD for OSPF on an IPv4 VLAN Interface

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable OSPF BFD on an IPv4 VLAN interface.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the navigation pane, expand **Configuration** > **VLAN**.
2. Select **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN on which you want to enable BFD for OSPF.
5. Select **IP**.
6. Select **OSPF**.
7. Select **BfdEnable**.

OSPF Field Descriptions

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

Name	Description
Enable	Enables or disables OSPF routing on the specified VLAN. The default is false.
HelloInterval	Specifies the length of time, in seconds, between the transmission of hello packets. This value must be the same for all routers attached to a common network. The default is 10 seconds. After you change the hello interval values, you must save the configuration file, and then restart the switch. After the switch restarts, it restores the values and checks for consistency.
RtrDeadInterval	Specifies the interval used by adjacent routers to determine if the router was removed from the network. This interval must be identical on all routers on the subnet and a minimum of four times the hello interval. To avoid interoperability issues, the RtrDeadInterval value for the OSPF interface needs to match with the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds.
DesigRtrPriority	Specifies the priority of this VLAN in multiaccess networks to use in the designated router election algorithm. The value 0 indicates the router is not eligible to become the designated router on this particular

Table continues…

Name	Description
	network. If a tie occurs, routers use their router ID as a tie breaker. The default is 1.
Metric	Specifies the metric for this TOS on this VLAN. The value of the TOS metric is (10^9 / interface speed). The default is 1. • FFFF—No route exists for this TOS. • IPCP links—Defaults to 0. • 0—Use the interface speed as the metric value when the state of the interface is up.
AuthType	Specifies the type of authentication required for the interface. • none—Specifies that no authentication required. • simple password—Specifies that all OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey parameter. • MD5 authentication—Specifies that all OSPF updates received by the interface must contain the MD5 key. • sha1—Specifies secure hash algorithm 1 (SHA-1), which is a cryptographic hash function that produces a 160-bit hash value, usually given in a hexadecimal number, 40 digits long. You can only access and enable the SHA-1 authentication type after you enable enhanced secure mode. • sha-2—Specifies SHA-2, which offers the hash function SHA-256. **Note:** sha-2, an update of SHA-1, can offer six hash functions that include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA 512/256, with hash values that are 224, 256, 384, or 512 bits. However, the current release supports only SHA-256.
AuthKey	Specifies the key (up to eight characters) when you specify simple password authentication in the VLAN AuthType variable.
AreaId	Specifies the OSPF area name in dotted-decimal format. The area name is not related to an IP address. You can use a suitable value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
AdvertiseWhenDown	Advertises the network even if the port is down. If true, OSPF advertises the network on this VLAN as up, even if the port is down. The default is false. After you configure a port without a link and enable AdvertiseWhenDown, it does not advertise the route until the port is active. Then, OSPF advertises the route even when the link is down. To disable advertising based on link states, disable AdvertiseWhenDown.

Table continues…

Name	Description
IfType	Specifies the type of OSPF interface (broadcast, NBMA, or passive). Before you change an OSPF interface type, you must first disable the interface. If the interface is an NBMA interface, you must also delete all configured neighbors.
PollInterval	Specifies the length of time, in seconds, between hello packets sent to an inactive OSPF router. Neighbors must use the same poll interval.
IfMtuIgnore	Specifies whether the VLAN ignores the MTU configuration. To allow the switch to accept OSPF DD packets with a different MTU size, enable MtuIgnore. The interface drops incoming OSPF DD packets if their MTU is greater than 1500 bytes.
BfdEnable	Enables Bidirectional Forwarding Detection (BFD) for OSPF.

Enable BFD for OSPF on an IPv6 Port Interface

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable BFD for the OSPF protocol on an IPv6 port interface.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation pane, expand **Configuration** > **Edit** > **Port**.
3. Select **IPv6**.
4. Select the **IPv6 OSPF Interface** tab.
5. Select **Insert**.
6. Select **BfdEnable**.

IPv6 OSPF Interface field descriptions

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

Name	Description
Index	Shows the interface index for the IPv6 interface on which OSPFv3 is configured.

Table continues…

Name	Description
AreaId	Specifies the area ID to which the IPv6 interface connects. Use 0.0.0.0 for the OSPFv3 backbone.
Type	Specifies the OSPFv3 interface type as one of the following: • broadcast • NBMA • point-to-point • point-to-multipoint • passive
AdminStat	Specifies the administrative status for the OSPFv3 interface. If you enable the status, it is advertised as an interal route to some areas. If you disable the status, the interface is external to OSPFv3. The default is enabled.
RtrPriority	Specifies the priority of this interface. Multiaccess networks use the priority in the designated router election. A higher priority value increases the chance the router becomes the designated router. A value of zero (0) indicates the router cannot become the designated router for the network. If more than one router uses the same priority value, the router ID determines the designated router. The default is 1.
TransitDelay	Specifies the estimated number of seconds to transmit a link-state-update packet over this interface. The default is 1.
RetransInterval	Specifies the number of seconds between retransmission of link-state advertisements for the adjacencies that belong to this interface, and for database description and link-state request packets. The default is 5.
HelloInterval	Specifies the number of seconds between the hello packets that the router sends on this interface. You must configure this field to the same value for all routers attached to a common network. The default is 10.
RtrDeadInterval	Specifies the number of seconds after which to declare a router down if no hello packets are received. You must configure this field to the same value for all routers attached to a common network. The default is 40.

Table continues…

Name	Description
PollInterval	Specifies the number of seconds between hello packets sent to an inactive NBMA neighbor. The default is 120.
State	Shows the state of the OSPFv3 interface as one of the following: • down • loopback • waiting • pointToPoint • designatedRouter • backupDesginatedRouter • otherDesignatedRouter
DesignatedRouter	Shows the router ID for the designated router.
BackupDesignatedRouter	Shows the router ID for the backup designated router.
MetricValue	Specifies the cost for the interface. The default value for a brouter port or VLAN is 1. The default value for a tunnel is 100. **Note:** If you do not specify a cost for the interface, the switch dynamically updates the interface cost with the configured global OSPF default cost. The global OSPF default cost depends on the speed of the interface.
LinkLsaSuppression	Specifies whether Link LSA suppression is enabled.
BfdEnable	Enable Bidirectional Forwarding Detection (BFD) for OSPF.

Enable BFD for OSPF on an IPv6 VLAN Interface

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

About this task

BFD provides a failure-detection mechanism between two systems. Use the following procedure to enable OSPF BFD on an IPv6 VLAN interface.

Note:
Enabling BFD at the application level does not establish a BFD session. To establish a BFD session, you must enable BFD globally and at the interface level.

Procedure

1. In the navigation pane, expand **Configuration** > **VLAN**.
2. Select **VLANs**.
3. Select the **Basic** tab.
4. Select the VLAN on which you want to enable BFD for OSPF.
5. Select **IPV6**.
6. Select **IPv6 OSPF Interface**.
7. Select **Insert**.
8. Select **BfdEnable**.

IPv6 OSPF Interface field descriptions

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

Name	Description
Index	Shows the interface index for the IPv6 interface on which OSPFv3 is configured.
AreaId	Specifies the area ID to which the IPv6 interface connects. Use 0.0.0.0 for the OSPFv3 backbone.
Type	Specifies the OSPFv3 interface type as one of the following: • broadcast • NBMA • point-to-point • point-to-multipoint • passive
AdminStat	Specifies the administrative status for the OSPFv3 interface. If you enable the status, it is advertised as an interal route to some areas. If you disable the status, the interface is external to OSPFv3. The default is enabled.
RtrPriority	Specifies the priority of this interface. Multiaccess networks use the priority in the designated router election. A higher priority value increases the chance the router becomes the designated router. A value of zero (0) indicates the router cannot become the designated router for the network. If more than one router uses the same priority value, the router ID determines the designated router.

Table continues…

Name	Description
	The default is 1.
TransitDelay	Specifies the estimated number of seconds to transmit a link-state-update packet over this interface. The default is 1.
RetransInterval	Specifies the number of seconds between retransmission of link-state advertisements for the adjacencies that belong to this interface, and for database description and link-state request packets. The default is 5.
HelloInterval	Specifies the number of seconds between the hello packets that the router sends on this interface. You must configure this field to the same value for all routers attached to a common network. The default is 10.
RtrDeadInterval	Specifies the number of seconds after which to declare a router down if no hello packets are received. You must configure this field to the same value for all routers attached to a common network. The default is 40.
PollInterval	Specifies the number of seconds between hello packets sent to an inactive NBMA neighbor. The default is 120.
State	Shows the state of the OSPFv3 interface as one of the following: • down • loopback • waiting • pointToPoint • designatedRouter • backupDesginatedRouter • otherDesignatedRouter
DesignatedRouter	Shows the router ID for the designated router.
BackupDesignatedRouter	Shows the router ID for the backup designated router.
MetricValue	Specifies the cost for the interface. The default value for a brouter port or VLAN is 1. The default value for a tunnel is 100. **Note:** If you do not specify a cost for the interface, the switch dynamically updates the interface cost

Table continues…

Name	Description
	with the configured global OSPF default cost. The global OSPF default cost depends on the speed of the interface.
LinkLsaSuppression	Specifies whether Link LSA suppression is enabled.
BfdEnable	Enables Bidirectional Forwarding Detection (BFD) for OSPF.

Configure BFD on an IPv4 Static Route

Procedure

1. In the navigation pane, expand **Configuration** > **IP**.
2. Select **BFD**.
3. Select **Insert**.
4. In the **NextHop** field, type the IPv4 address of the next hop of the BFD session.
5. **(Optional)** In the **VrfId** field, type the ID of the VRF associated with the BFD session.

BFD Static Route Field Descriptions

Use the data in the following table to use the Static Route tab.

Name	Description
NextHop	Specifies the IPv4 address of the next hop of the BFD session.
VrfId	Specifies the ID of the VRF associated with the BFD session.
VrfName	Specifies the name of the VRF associated with the BFD session.

Configure BFD on an IPv6 Static Route

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

Procedure

1. In the navigation pane, expand **Configuration** > **IPv6**.
2. Select **IPv6 BFD**.
3. Select **Insert**.
4. In the **Interface** field, select either **Port** or **Vlan** and select an interface.

5. In the **NextHop** field, type the IPv6 address of the next hop of the BFD session.
6. **(Optional)** In the **VrfId** field, type the ID of the VRF associated with the BFD session.

IPv6 BFD Static Route Field Descriptions

Use the data in the following table to use the Static Route tab.

Name	Description
Interface	Specifies either a port or VLAN interface.
NextHop	Specifies the IPv4 address of the next hop of the BFD session.
VrfId	Specifies the ID of the VRF associated with the BFD session.
VrfName	Specifies the name of the VRF associated with the BFD session.

Display BFD Performance Counters

BFD for IPv6 interfaces is a demonstration feature on some products. For more information about feature support, see VOSS Feature Support Matrix.

Procedure

1. In the navigation pane, expand **Configuration** > **Edit**.
2. Select **BFD**.
3. Select the **Performance counters** tab.

BFDPerformance Counters Field Descriptions

Use the data in the following table to use the Performance counters tab.

Name	Description
PktIn	Specifies the total number of BFD messages received for this BFD session.
PktOut	Specifies the total number of BFD messages sent for this BFD session.

Chapter 19: 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 531.

The following table shows the default values for login and password for the console and Telnet sessions.

Table 53: 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 mode boot configuration 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 for VOSS.

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 531.

Default web-server behavior

The default switch configuration enforces the following restrictions for web-server access:

- The web-server password must be a minimum of 8 characters.
- Secure communications with the web server use Transport Layer Security (TLS) version 1.2 and above.
- The switch does not support the RC4 cipher. The switch supports the following ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256

For information about how to enable and configure the web server, including supported browser versions, see Configuring User Interfaces and Operating Systems for VOSS.

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 for VOSS.

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 Remote login (rlogin) sessions.

Note:

Rlogin is only supported on VSP 8600 Series.

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.

Note:

Rlogin is only supported on VSP 8600 Series.

Use access policies for in-band management to secure access to the switch. When configuring an access policy, a lower precedence takes higher priority if you use multiple policies. For example, 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 Configuring User Interfaces and Operating Systems for VOSS.

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.

By default, the minimum password length for the web server is 8 characters but you can override this value. For more information about how to enable and configure the web server, including username and password configuration, see Configuring User Interfaces and Operating Systems for VOSS.

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.

Multiple CLI Users for Each Role

Table 54: Multiple CLI Users product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Multiple CLI users per role	VSP 4450 Series	VOSS 7.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 7.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 7.0
	VSP 8400 Series	VOSS 7.0
	VSP 8600 Series	VSP 8600 8.0 demonstration feature
	XA1400 Series	VOSS 8.0.50

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to a maximum of 10 CLI users for each role, which includes:

- 3 default users (rwa, rw, and ro)—User Type = default
- 7 user defined users (rwa or rw or ro)—User Type = userDefined

Usernames for default users (rwa, rw, and ro) can be changed; however, usernames for user defined users cannot be changed.

Users require a username and password to connect to the switch. Users can log on through the local serial port, Telnet, SSH, remote login (rlogin), or ftp. When a user is created, authentication is enabled, by default.

Note:

Rlogin is only supported on VSP 8600 Series.

For security reasons, if a login attempt fails, the error feedback does not indicate if the failed login is due to an invalid user name or an invalid password. Response times for invalid user name and invalid user name/password pair are identical to prevent identification of which of the two failed.

Note:

Multiple CLI users for each role does not apply in enhanced secure mode.

Enhanced secure mode authentication access levels

Table 55: Enhanced Secure Mode product support

Feature	Product	Release introduced
For configuration details, see Administering VOSS.		
Enhanced Secure mode	VSP 4450 Series	VOSS 4.2
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.2
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	Not Supported
	XA1400 Series	VOSS 8.0.50
Enhanced Secure mode for JITC and non-JITC sub-modes.	VSP 4450 Series	VOSS 5.1
	VSP 4900 Series	VOSS 8.1

Table continues…

Feature	Product	Release introduced
	VSP 7200 Series	VOSS 5.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 5.1
	VSP 8400 Series	VOSS 5.1
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

After you enable enhanced secure mode with the **`boot config flags enhancedsecure-mode`** command, the switch supports role-based authentication levels. With enhanced secure mode enabled, the switch supports the following authentication access levels for local authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

Each username is associated with a certain role in the product and appropriate authorization rights for viewing and executing commands are available for that role.

With enhanced secure mode enabled, the person in the role-based authentication level of administrator configures the login and password values for the other role-based authentication levels.

The administrator initially logs on to the switch using the default login of `admin` and the default password of `admin`. After the initial login, the switch prompts the administrator to create a new password.

The following displays an example of the initial login to the switch by the administrator after enhanced secure mode is enabled.

```
Login: admin
Password: *****
        This is an initial attempt using the default user name and password.
        Please change the user name and password to continue.
Enter the new name : rwa
Enter the New password : ****************
Re-enter the New password : ****************
Password changed successfully
        Last Successful Login:Wed Oct 14 12:20:42 2015
         Unsuccessful Login attempts from last login is: 0
```

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user.

Access level and login details

Access level	Description	Login location
Administrator	The administrator access level permits all read-write access, and can change security settings. The administrator access level can configure CLI and web-based management user names, passwords, and the SNMP community strings. The administrator access level can also view audit logs.	SSH/Telnet (in band/mgmt)/ console
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

The following table defines parameters for 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

The following table defines parameters for 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.

Configure 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

The following table defines parameters for 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 **Note:** Exception: only supported on VSP 8600 Series.	Enables rlogin for the access policy.

Table continues…

Variable	Value
snmp-group *WORD<1–32>* <snmpv1|snmpv2c|usm>	Adds an SNMP version 3 group under the access policy. *WORD<1–32>* is the SNMP version 3 group name consisting of 1–32 characters. <snmpv1|snmpv2c|usm> is the security model; either snmpv1, snmpv2c, or usm. Use the no operator to remove this configuration.
snmpv3	Activates SNMP version 3 for the access policy. Use the no operator to remove this configuration.
ssh	Activates SSH for the access policy. 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

The following table defines parameters for 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

The following table defines parameters for 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. 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

The following table defines parameters for 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.

Creating multiple CLI users

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to seven new CLI users on the switch, in addition to the three default CLI users. The username must be unique. If you enable the hsecure flag, password complexity rules apply to all users.

Before you begin

You must use an account with read-write-all privileges to create new CLI users.

About this task

Note:

When a new CLI user is created, the specified username and access level cannot be changed later.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a new CLI user:

   ```
   username add {<WORD 1-20> level [ro|rw|rwa] enable}
   ```

3. Enter a password.
4. Enter the password a second time.

Example

Create a new CLI user:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#username add smith level rwa enable
Enter password : *******
Re-enter password : *******
Switch:1(config)#
```

Variable Definitions

The following table defines parameters for the **`username`** command.

Variable	Value
add *WORD<1–20>*	Specifies the username to create.
enable	Enables the new CLI user.
level <*ro* | *rw* | *rwa*>	Specifies the level assigned to the new CLI user: • ro: Read-only level • rw: Read-write level • rwa: Read-write-all level

Deleting a username

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to delete a username. Default ro, rw, and rwa users cannot be deleted.

Before you begin

You must use an account with read-write-all privileges to delete a user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete the username:

   ```
   no username <WORD 1-20>
   ```

Example

Delete a user:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#no username smith
The specified username will be deleted! Contiune (y/n) ? Y
Switch:1(config)#show cli username smith
Username does not exit
```

Variable Definitions

The following table defines parameters for the **no username** command.

Variable	Value
WORD <1–20>	Specifies the username to delete.
enable	Disables the username.

Displaying CLI usernames and roles

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to display CLI usernames and roles.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display CLI usernames and roles:

   `show cli username`

Example

```
Switch:1>show cli username

=============================================================
UserName              AccessLevel    State        Type
=============================================================
ro                    ro             enable       default
rw                    rw             enable       default
rwa                   rwa            NA           default
smith                 rw             enable       userDefined
```

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 flags status:

```
show boot config flags
```

Example

In the following example, the status displays that enhanced secure mode is disabled.

Note:

Flag support can vary across hardware models.

```
Switch:1#show boot config flags
flags advanced-feature-bandwidth-reservation low
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 true
flags ha-cpu true
flags hsecure false
flags ipv6-egress-filter true
flags ipv6-mode false
flags linerate-directed-broadcast false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags savetostandby true
flags spanning-tree-mode mstp
flags spbm-config-mode true
flags sshd true
flags syslog-rfc5424-format true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode true
flags verify-config true
flags vrf-scaling true
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.
user *WORD<1–255>*	Specifies a particular user.

Configuring the Pre-notification 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:

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.

Configuring CLI Access using EDM

Use the following procedures to perform CLI access configuration tasks such as:

- Enable access levels
- Change passwords
- Configure the logon banner

Enable 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 **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **CLI** tab.

4. Select the enable check box for the required access level.
5. Click **Apply**.

Change 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**Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Specify the username and password for the appropriate access level.
5. Click **Apply**.

Configure the Logon Banner

About this task

Configure the logon banner using EDM to display a warning message to users on the CLI before authentication.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click General.
3. Click the CLI tab.
4. Enter the banner text in the **CustomBannerText** field.
5. Check the **CustomBannerEnable** check box.
6. Click **Apply**.

CLI Field Descriptions

The following table defines parameters for 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.

Table continues…

Name	Description
RWL3Enable	Activates the read-write Layer 3 access. The default is enabled.
RWL3UserName	Specifies the user name for the Layer 3 read-write CLI account.
RWL3Password	Specifies the password for the Layer 3 read-write CLI account.
RWL2Enable	Activates the read-write Layer 2 access. The default is enabled.
RWL2UserName	Specifies the user name for the Layer 2 read-write CLI account.
RWL2Password	Specifies the password for the Layer 2 read-write CLI account.
RWL1Enable	Activates the read-write Layer 1 access. The default is enabled.
RWL1UserName	Specifies the user name for the Layer 1 read-write CLI account.
RWL1Password	Specifies the password for the Layer 1 read-write CLI account.
ROEnable	Activates the read-only CLI account. The default is enabled.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Specifies the maximum number of concurrent Telnet sessions in a range from 0–8. The default is 8.
MaxRloginSessions	Specifies the maximum number of concurrent rlogin sessions in a range from 0–8. The default is 8.
Timeout	Specifies the number of seconds of inactivity for a Telnet or Rlogin session before the system initiates automatic timeout and disconnect, expressed in a range from 30–65535. The default is 900 seconds.
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This variable is a read-only field.
CustomBannerText **Note:** Exception: not supported on VSP 8600 Series.	Specifies the text message that is displayed to users on the CLI before authentication. The message can be company information, such as company name and contact, or a warning message for the users of CLI. With character limitation from 1-1800, the text box displays 79 characters per line.
CustomBannerEnable **Note:** Exception: not supported on VSP 8600 Series.	Specifies whether custom logon banner is enabled or disabled. The default is enabled.

Create 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.

Note:

Rlogin is only supported on VSP 8600 Series.

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.

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 **Configuration** > **Security** > **Control Path**.
2. Select **Access Policies**.
3. Select the **Access Policies** tab.
4. Select **Insert**.
5. In **ID**, type the policy ID.
6. In **Name**, type the policy name.
7. Select **PolicyEnable**.
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 **Precedence**, type a precedence number for the service (lower numbers mean higher precedence).
11. Select the **NetInetAddrType**.
12. In **NetInetAddress**, type an IP address.
13. In **NetInetAddrPrefixLen**, type the prefix length.
14. In **TrustedHostInet Address**, type an IP address for the trusted host.
15. In **TrustedHostUserName**, type a user name for the trusted host.
16. Select an **AccessLevel** for the service.
17. Select **AccessStrict**, if required.

Important:

If you select **AccessStrict**, you specify that a user must use an access level identical to the one you select.

18. Select **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

Table continues…

Name	Description
	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 ✱ **Note:** Exception: rlogin and rsh are only supported on VSP 8600 Series.	Indicates the trusted Inet address of a host performing a remote login to the device. You do not need to provide this information if you select the NetInetAddrType of any. TrustedHostInetAddr applies only to rlogin and rsh. **!** **Important:** You cannot use wildcard entries in the TrustedHostInetAddr field. If the type is IPv4, you must enter an IPv4 address and mask length. If the type is IPv6, you must enter an IPv6 address and prefix length.
TrustedHostUserName ✱ **Note:** Exception: rlogin and rsh are only supported on VSP 8600 Series.	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 ✱ **Note:** If **Mode** is configured as **allow** the system checks **AccessStrict** information. If **Mode** is configured as **deny**, the system does not check **AccessStrict** information.

Table continues…

Name	Description
	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).

Enable 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).

Note:

Rlogin is only supported only on VSP 8600 Series.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation pane, expand **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. Select the **EnableAccessPolicy** check box.
6. Click **Apply**.

Creating Multiple Users

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

You can create up to seven new CLI user roles on the switch, in addition to the three default CLI user roles. The username must be unique. If you enable the hsecure flag, password complexity rules apply to all users.

Before you begin

You must use an EDM account with read-write-all privileges to create new CLI users.

About this task

Use this task to create multiple CLI users on the switch using EDM.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. Click **Insert**.
5. Type the ID.
6. Type a unique user name.
7. Type a password.
8. Select the access level.
9. Select **Enable** to activate the user account.
10. Click **Insert**.

Multiple Users field descriptions

Use the data in the following table to the use the Multiple Users tab.

Name	Description
Id	Specifies the unique ID.
Name	Specifies the username.
Password	Specifies the password.
Level	Specifies the user access level. • ro • rw • rwa
Enable	Enables the user access on the switch.
Type	Specifies the user type.

Modify User Passwords

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to modify user account passwords using EDM.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. To change the user account password, double-click the **Password** field.
5. Click **Apply**.

Disable a User Account

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to disable a user account using EDM.

Note:

Users with rwa access rights cannot be disabled. Only users with ro and rw access rights can be disabled.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. View whether the user account is enabled. To modify, double-click on the cell and select false from the list.
5. Click **Apply**.

Delete a User Account

About this task

Note:

DEMO FEATURE - Multiple CLI Users Per Role is a demonstration feature on some products. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment. For more information on feature support, see VOSS Feature Support Matrix.

Use this task to delete a user account using EDM. You cannot delete default ro, rw, and rwa users.

Procedure

1. In the navigation pane, expand **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Multiple Users** tab.
4. Select the row with the user account to delete and click **Delete**.
5. Click **Yes** to confirm.

System access security enhancements using EDM

The section provides information to enable enhanced secure mode.

Enable 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 **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Boot Config** tab.
5. In the **EnableEnhancedsecureMode** option box, select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. Select **disable** to disable the enhanced secure mode.

   ✻ **Note:**

   It is recommended that you enable the non-JITC sub-mode. The JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
6. Click **Apply**.
7. Save the configuration, and restart the switch.

Chapter 20: 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
        l3        l3               ena
        l2        l2               ena
        l1        l1               ena
        Default Lockout Time       60
        Default Lockout Retries        3
        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 <app-telemetry | boot | cfm | cli | diag | dvr | eap | endpoint-tracking | energy-saver | fa | fhs | filter | ike | ip | ipfix | ipsec | ipv6 | iqagent | isis | i-sid | lacp | license | lldp | lst | macsec | mlt | naap | nls | ntp | ovsdb | port | qos | radius | restconf | rmon | sflow | security | slamon | slpp | smtp | spbm | stg | sys | tacacs | virtualservice | vlan | web | vxlan>]

The following table explains parameters for this command.

Table 56: Command parameters

Parameter	Description
module <app-telemetry | boot | cfm | cli | diag | dvr | eap | endpoint-tracking | energy-saver | fa | fhs | filter | ike | ip | ipfix | ipsec | ipv6 | iqagent | isis | i-sid | lacp | license | lldp | lst | macsec | mlt | naap | nls | ntp | ovsdb | port | qos | radius | restconf | rmon | sflow | security | slamon | slpp | smtp | spbm | stg | sys | tacacs | virtualservice | 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 Dec 18 14:04:23 2016 UTC
# box type              : VSP-8608
# software version      : 4.5.0.0
# 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.

Command output can vary across hardware models.

```
Switch:1#show cli info

cli configuration
```

```
more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:
prompt : 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

To display system status and technical information about the switch hardware components, use the **show sys-info** command. The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), cpld, temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information.

You can identify a port-licensed 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 Virtual Services Platform 7200 Series.

The syntax for this command is as follows:

show sys-info {card | cpld | fan | led | power | ssd | temperature | uboot | usb}

The following table defines parameters for the **show sys-info** command.

Table 57: Command parameters

Parameter	Description
card	Specifies information about the device. Includes type, serial number, and assembly date. **Note:** Not all hardware platforms support removable cards or modules. If a platform does not support removable cards or modules, the output provides information on the chassis as a whole. For more information, see the hardware documentation for your platform.
cpld	Specifies information about field programmable gate arrays (FPGA) and complex programmable logic devices (CPLD). **Note:** This parameter is not supported on all hardware platforms.
fan	Specifies information about installed cooling ports.
led	Specifies LED information in detail.
power	Specifies information about installed power supplies.
ssd	Specifies information about installed modular Solid State Drives (SSD). **Note:** This parameter is not supported on all hardware platforms.
temperature	Specifies temperature information.
uboot	Specifies uboot details.
usb	Specifies information about cached USB information.

The following examples show partial output from the **`show sys-info`** command for various switches. The output for this command will vary on switches because of hardware differences.

The following example shows partial output from the **`show sys-info`** command for a VSP 8284XSQ switch.

```
Switch:1>show sys-info

General Info :

        SysDescr      : VSP-8284XSQ (w.x.y.z)
        SysName       : Switch
        SysUpTime     : 0 day(s), 15:49:09
        SysContact    : http://www.extremenetworks.com/contact/
        SysLocation   : 9 Northeastern Blvd,Salem,NH. 03079

Chassis Info:
        Chassis            : 8284XSQ
        ModelName          : 8284XSQ
        BrandName          : Extreme Networks
        Serial#            : 14JP174C1013
        H/W Revision       : 1
        H/W Config         :
        Part Number        : EC8200A01-E6
        NumSlots           : 2
        NumPorts           : 85
        BaseMacAddr        : b0:ad:aa:43:48:00
        MacAddrCapacity    : 1024
        MgmtMacAddr        : b0:ad:aa:43:48:81
        System MTU         : 1950

Card Info :

        Slot#      CardType          Serial#            Part#             Oper     Admin
Power
                                                                        Status    Status
State
            1       8242XSQ     14JP174C1013     EC8200A01-E6                up
up     on
            2       8242XSQ     14JP174C1013     EC8200A01-E6                up
up     on

Temperature Info :


    CPU Temperature    MAC Temperature   PHY1 Temperature   PHY2 Temperature

                  33                 36                 29                 34




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        : 5
        Max-msg-num             : 5
        Status                  : disable




Configuration Operation Info :

         Last Change: 0 day(s), 00:03:30
    Last Vlan Change: 0 day(s), 00:03:30
Last Statistic Reset: 0 day(s), 00:00:00


Current Uboot Info :
------------------------------------------------------------------------------------------
----------

 VU-Boot 2012.04-00002-g6fb1c26 (Apr 26 2017 - 13:51:26) bld=17042617
```

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 (w.x.y.z)
        SysName      : SF-237:1
        SysUpTime    : 9 day(s), 00:30:59
        SysContact   : support@extremenetworks.com
        SysLocation  :
```

```
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
```

The following example shows partial output from the **`show sys-info`** command for a VSP4900-12MXU-12XE switch.

```
Switch:1>show sys-info

General Info :

        SysDescr     : VSP-4900-12MXU-12XE (w.x.y.z)
        SysName      : Switch
        SysUpTime    : 1 day(s), 06:14:14
        SysContact   : http://www.extremenetworks.com/contact/
        SysLocation  :

Chassis Info:

        Chassis            : VSP-4900-12MXU-12XE
        ModelName          : VSP-4900-12MXU-12XE
        BrandName          : Extreme Networks.
        Serial#            : 1924F-10300
        H/W Revision       : 01
        H/W Config         :
        Part Number        : 800977-00-01
        NumSlots           : 2
        NumPorts           : 27

        BaseMacAddr        : b0:ad:aa:43:48:00
        MacAddrCapacity    : 1024
        MgmtMacAddr        : b0:ad:aa:43:48:81
        System MTU         : 1950

Card Info :

 Slot#       CardType          Serial#            Part#            Oper   Admin  Power
                                                                  Status  Status  State
  1      VSP4900-12MXU-12XE  19000-10396       800977-00-01          up      up     on

Temperature Info :

              Sensor                  Warning   Critical
         Description   Temperature  Threshold  Threshold
                 CPU            40         78         86
        MAIN BOARD 1            44         57         62
        MAIN BOARD 2            43         59         64
            CPU CORE            32         75         95
                 MAC            69        100        110
                PHY1            41        100        110
                PHY2            40        100        110
                PHY3            43        100        110

                PHY4            50        100        110
                PHY5            53        100        110
                PHY6            53        100        110


Power Supply Info :

        Ps#1 Status       : UP
        Ps#1 Type         : AC
        Ps#1 Description  : Summit 350W AC PSU
        Ps#1 Serial Number: 2400
        Ps#1 Version      : 07
        Ps#1 Part Number  : 800764-00-07

        Ps#2 Status       : empty

        Total Power Available : 350 watts
        Total Power Usage     : 330 watts

Fan Info :

            Description   OperStatus       OperSpeed   AirflowDir
           Tray 1 Fan 1           up        lowSpeed   front-back
           Tray 1 Fan 2           up        lowSpeed   front-back
           Tray 2 Fan 1           up        lowSpeed   front-back
           Tray 2 Fan 2           up        lowSpeed   front-back
           Tray 3 Fan 1           up        lowSpeed   front-back
           Tray 3 Fan 2           up        lowSpeed   front-back

SSD Module Info:
        Product Name      : XN-SSD-001-120
        Vendor Name       : Extreme Networks Inc.
        Manufacture Date  : 09/06/2019 18:16:38
        Serial Num        : 1936F-10000
        Part Num          : 800954-00-AA
        Device Version    : 0
        Total Size        : 120GB


LED Info :

        LED#1 Label  : SYS
        LED#1 Status : GreenSteady

        LED#2 Label  : SPD
        LED#2 Status : Off

        LED#3 Label  : STK
        LED#3 Status : Off

        LED#4 Label  : BT
        LED#4 Status : Off

        LED#5 Label  : P1
        LED#5 Status : GreenSteady

        LED#6 Label  : P2
        LED#6 Status : Off

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       : 5

        Max-msg-num            : 5
        Status                 : disable

Configuration Operation Info Since Boot Up:
         Last Change: 0 day(s), 00:01:41   (1 day(s), 06:13:22 ago)
    Last Vlan Change: 0 day(s), 00:00:00
Last Statistic Reset: 0 day(s), 00:00:00

Current FPGA/CPLD Info :

         MODULE                  VERSION

         CPU CPLD                : 1.1.18
         SYSTEM FPGA             : 1.2.41
         PORT1 PLD               : 1.1.08
```

To display port information for a switch, use the **show interfaces gigabitethernet** command.

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
```

High Availability State

Use the **show ha-state** command to view detailed information on High Availability (HA) state of the system.

The syntax for this command is as follows.

show ha-state

The following example shows sample command output.

```
Switch:1(config)#show ha-state
Current CPU State : Initialization state.
```

Note:

Use the **show sys-info** command to view the slots of the master CPU and the standby CPU. You can also check whether the standby CPU is running in hot standby mode or warm standby mode.

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: redundant

             Total     Required  Max
Chassis      Chassis   Redundant Allocated Available Reserved Required
Type         Power     Power     Power     Power     Power    Power
------------------------------------------------------------------------------------------
SwitchXYZ     4200      1400      1851      2349      1411     1851
------------------------------------------------------------------------------------------
```

Note:

Power information can differ by hardware platform. For more information, see the hardware documentation for your platform.

Power management information

Use the **show sys power global** command to view a summary of the power redundancy settings.

The syntax for this command is as follows.

show sys power global

The output varies according to platform. The following example shows sample command output for one hardware platform.

```
Switch:1#show sys power global
              slot 1     : critical
              slot 2     : critical
              slot 3     : high
              slot 4     : high
              slot 5     : high
              slot 6     : high
              slot 7     : high
              slot 8     : high
              slot SF1   : critical
              slot SF2   : critical
              slot SF3   : critical
```

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.

Slot power details

Use the **`show sys power slot`** command to view detailed power information for each slot.

The syntax for this command is as follows.

`show sys power slot`

The following example shows sample command output.

```
Switch:1#show sys power slot

================================================================================
                             Slot Power Consumption
================================================================================
                                                        Max
Slot     Present CardType            Priority    Power  Allocated
No.                                              Status Power
--------------------------------------------------------------------------------
1        YES     8624XS              CRITICAL    ON     310
2        YES     8624XS              CRITICAL    ON     310
```

```
3        YES     8624XT              HIGH        ON     347
4        NO      Not Present         HIGH        OFF    0
5        YES     8606CQ              HIGH        ON     292
6        YES     8606CQ              LOW         ON     292
7        NO      Not Present         HIGH        OFF    0
8        NO      Not Present         HIGH        OFF    0
SF 1     YES     8600SF              CRITICAL    ON     157
SF 1     YES     8600SF              CRITICAL    ON     157
SF 1     YES     8600SF              CRITICAL    ON     157
--------------------------------------------------------------------------------

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

System Information

Use the **`show sys`** command to display system status and technical information about the switch hardware components and software configuration. The command shows several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information. The syntax for this command is as follows.

`show sys <control|dns|force-msg|locator-led|mgid-usage|msg-control|mtu|power|priv-exec-password|setting|software|stats|topology-ip|vim-speed>`

The following table explains parameters for this command.

Table 58: Command parameters

Parameter	Description
control	Shows system control settings.
default-ping-context	Specifies the default context for ping and traceroute commands.
dns	Shows the DNS default domain name.
force-msg	Shows the message control force message pattern settings.
locator-led	Shows the locator LED status.
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: • global—power management settings

Table continues…

Parameter	Description
	• power-supply—power information for each power supply • slot—power information for each slot
priv-exec-password	Shows whether authentication is enabled for the Privileged EXEC CLI command mode.
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 for VOSS. This parameter does not apply to all hardware platforms.
topology-ip	Shows the circuitless IP set.
vim-speed	Shows the speed of all ports of the VIM.

The following example shows output from the **show sys control** command.

```
Switch:1>show sys control
==========================================================================================
==========
                            System Control Settings
==========================================================================================
==========
                 tcp-timestamp : enable
            tcp-keepalive-time : 60
        tcp-keepalive-interval : 10
          tcp-keepalive-probes : 5
```

Note:
The tcp-keepalive-time, tcp-keepalive-interval, and tcp-keepalive-probes fields are not supported on VSP 8600 Series.

The following example shows output from the **show sys dns** command. The same output applies from the **show ip dns** command.

```
Switch:1>show sys dns
    DNS Default Domain Name : test.company.com
    DNS Default Domain Name Origin: DHCP
    DNS Host Name: voss10cdae6bd000
    Primary dynamic DNS server details:
    ===========================
         IP address : 192.0.2.11
         Status     : active
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0

    Secondary dynamic DNS server details:
    ===========================
         IP address : 192.0.2.12
         Status     : active
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
```

```
       Tertiary dynamic DNS server details:
    ===========================
         IP address : 192.0.2.13
         Status     : active
         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://www.company.com/
               location : Anywhere, USA
                   name : Switch
               portlock : off
    sendAuthenticationTrap : false
           autotopology : on
                    mtu : 1950
              prototype : disable
     data-path-fault-shutdown : enable
            secure-console : disable
      default-ping-context : grt
```

Note:
The default-ping-context field is not supported on VSP 8600 Series.

The following example shows output from the **show sys software** command.

Command output can vary across hardware models.

```
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
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : false
```

The following example shows output from the **show sys priv-exec-password** command.

```
Switch:1#show sys priv-exec-password
           Privileged exec password status : enabled
```

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   : support@extremenetworks.com
        SysLocation  :

Chassis Info:

        Chassis            : 8284XSQ
        ModelName          : 8284XSQ
        BrandName          : Extreme Networks
        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]] [,...]}*

Note:

The show output displays either unicast packet stats for each port or all stats based on your hardware platform.

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#
```

The following example shows output that displays unicast packet stats for each ports:

```
Switch:1#show qos cosq-stats interface
================================================================================
                           QOS Cos Queue Stats Table
================================================================================
                          Port:1/1  QOS Known Unicast CoS Queue Stats
================================================================================
CoS  Accepted Packets  Accepted 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
================================================================================
                          Port:1/2   QOS Known Unicast CoS Queue Stats
================================================================================
CoS  Accepted Packets     Accepted 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

================================================================================
                          Port:1/3   QOS Known Unicast CoS Queue Stats
================================================================================
CoS  Accepted Packets     Accepted Bytes       Drop Packets         Drop Bytes
0    0                    0                    0                    0
1    1622                 124894               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    331                  46671                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

Note:

The first column of the show output can display either protocol type or show queue number depending on your hardware platform.

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
```

The following example shows output where the first column displays the protocol type.

Note:

Command output can vary across hardware models.

```
Switch:1#show qos cosq-stats cpu-port

==========================================================================================
                       QOS CoS Queue Cpu Port Stats Table

==========================================================================================
Protocol             Accepted Packets     Accepted Bytes       Drop Packets         Drop
Bytes
vrrp                 0                    0                    0                    0
vlacp                0                    0                    0                    0
lacp                 0                    0                    0                    0
cfm                  0                    0                    0                    0
vrrp_v6              0                    0                    0                    0
ist_ctl              0                    0                    0                    0
```

```
radius               0                    0                    0                    0
ntp                  0                    0                    0                    0
icmpv4               0                    0                    0                    0
slpp                 0                    0                    0                    0
bpdu                 0                    0                    0                    0
tdp                  39996                2559744              0                    0
eap                  0                    0                    0                    0
lldp                 8066                 1233184              0                    0
nd_mc_v6             0                    0                    0                    0
nd_uc_v6             0                    0                    0                    0
rlogin               0                    0                    0                    0
frag_uc_v6           0                    0                    0                    0
isis                 0                    0                    0                    0
ospf_mc              8401                 783178               0                    0
dhcp                 0                    0                    0                    0
pim_mc               0                    0                    0                    0
arp_request          3                    204                  0                    0
arp_reply            0                    0                    0                    0
rarp_request         0                    0                    0                    0
rarp_reply           0                    0                    0                    0
icmpv4_bc            0                    0                    0                    0
ospfv6_mc            0                    0                    0                    0
ftp                  0                    0                    0                    0
tftp                 0                    0                    0                    0
snmp                 0                    0                    0                    0
telnet               0                    0                    0                    0
ssh                  0                    0                    0                    0
rsh                  0                    0                    0                    0
http                 0                    0                    0                    0
dns                  0                    0                    0                    0
icmp_mc_v6           0                    0                    0                    0
icmp_uc_v6           0                    0                    0                    0
ipmc_data            0                    0                    0                    0
bgp                  0                    0                    0                    0
igmp                 0                    0                    0                    0
mld                  0                    0                    0                    0
pim_uc               0                    0                    0                    0
ospf_uc              0                    0                    0                    0
ospf_v6_uc           0                    0                    0                    0
hop_by_hop           0                    0                    0                    0
rip_v1               0                    0                    0                    0
rip_v2               0                    0                    0                    0
rip_v6               0                    0                    0                    0
mac_learning         0                    0                    0                    0
internal 1           0                    0                    0                    0
data_exception       131                  13386                0                    0
ttl_exception        0                    0                    0                    0
frag_mc_v6           0                    0                    0                    0
internal 2           0                    0                    0                    0
ipfix                0                    0                    0                    0
Switch:1#
```

Chapter 21: 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.

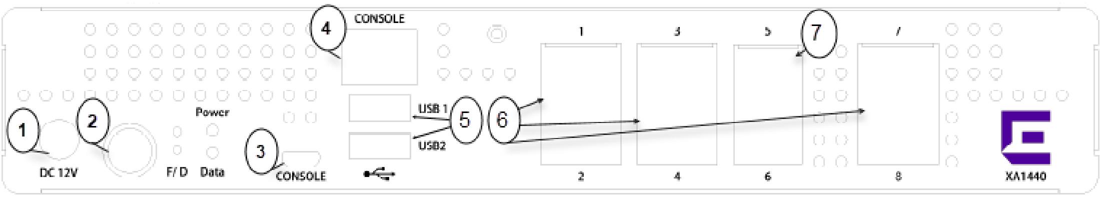
Port Numbering

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.

XA1400 Series

XA1440 and XA1480 Switches

The following figure illustrates the components on the rear panel of the XA1440 and XA1480. Slot 1 is used for all of the ports.



1 = DC power adapter input	3 = Micro USB console port	5 = USB Type A ports	7 = 10G SFP+ Ethernet ports
2 = Power button	4 = RJ45 Console port	6 = 10/100/1000BASE-T Ethernet ports	

Figure 9: XA1400 Series Switches Rear Panel

The rear panel components of XA1400 Series switches include:

- Power button

- 6 RJ45 10/100/1000BASE-T Ethernet ports.
- 2 10-gigabit Ethernet ports capable of supporting active fiber SFP+. For information about SFP + optical modules, see the *Extreme Networks Pluggable Transceivers Installation Guide*.
- RJ45 console port used to connect a terminal and perform local management.
- 2 USB ports for access to external storage.
- 1 MicroUSB console port used to connect a terminal and perform local management..

VSP 4000 Series

The following diagrams illustrate the components on the front panels of the VSP 4000 Series switches. Ethernet ports 1-50 on the switch are considered to be in slot 1.

VSP 4850GTS

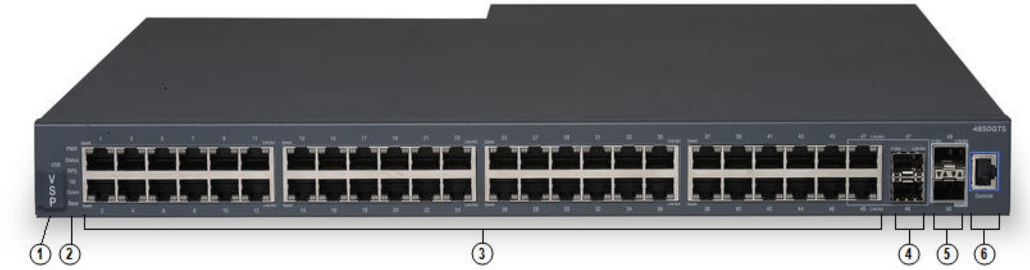


Figure 10: VSP 4850GTS

1. VSP 4000 USB cover.
2. Switch LEDs for system power (PWR), switch status (Status), and redundant power supply (RPS).
3. 48 10/100/1000 Mbps RJ-45 ports. LEDs indicating port activity are above the ports.
4. Two combo SFP ports. Supports 1G SFPs and 100Base low speed SFPs.
5. Two SFP+ ports. Supports 1G SFPs and 10G SFP+s.
6. Console Port

VSP 4850GTS-PWR+

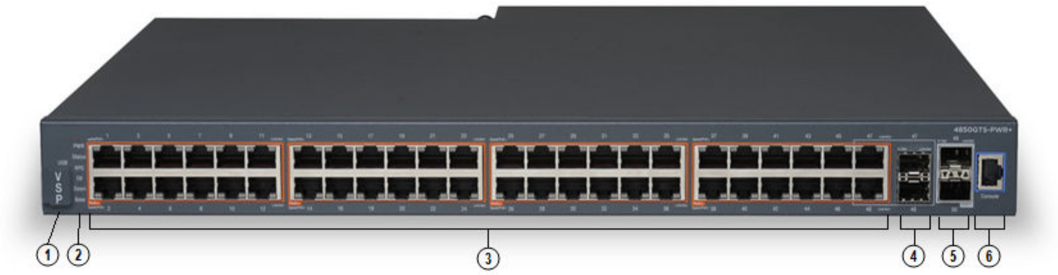


Figure 11: VSP 4850GTS-PWR+

1. VSP 4000 USB cover.
2. Switch LEDs for system power (PWR), switch status (Status), and redundant power supply (RPS)
3. 48 10/100/1000 Mbps PoE+ ports. LEDs indicating port activity are above the ports.
4. Two combo SFP ports. Supports 1G SFPs and 100Base low speed SFPs.
5. Two SFP+ ports. Supports 1G SFPs and 10G SFP+s.
6. Console Port.

VSP 4450GSX-PWR+

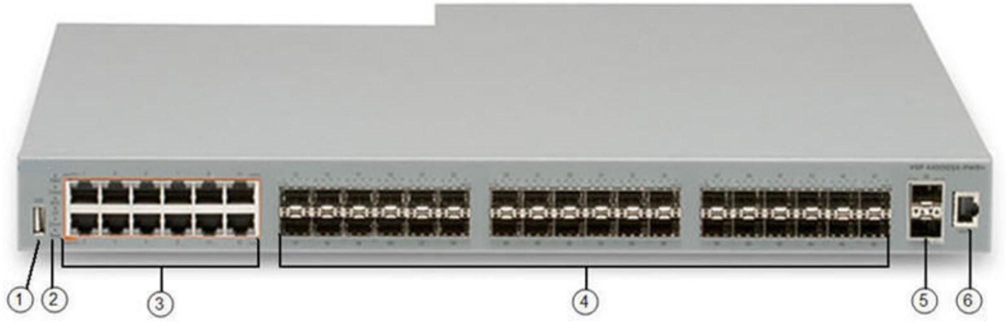


Figure 12: VSP 4450GSX-PWR+

1. VSP 4000 USB port.
2. Switch LEDs for system power (PWR), switch status (Status), and redundant power supply (RPS).
3. 12 10/100/1000 Mbps RJ-45 ports with PoE+. LEDs indicating port activity are above the ports.
4. 36 100/1000 Mbps SFP ports.
5. Two 1/10G SFP+ ports.
6. Console Port.

VSP 4450GTX-HT-PWR+

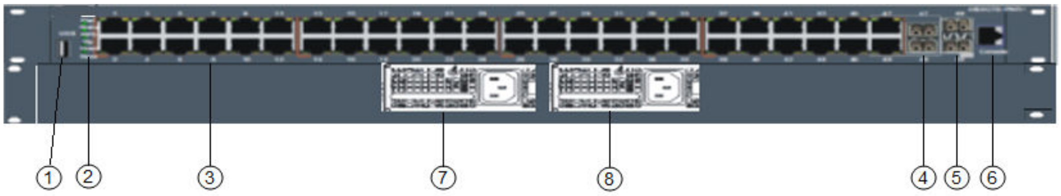


Figure 13: VSP 4450GTX-HT-PWR+

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 for system power (PWR), switch status (Status), and redundant power supply (RPS).
3. 48 10/100/1000 Mbps RJ-45 ports with 802.3at PoE+. LEDs indicating port activity are above the ports.
4. Two combo port SFP slots. Supports 1G SFPs and 100Base low speed SFPs.
5. Two SFP+ slots. Supports 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.

VSP 4450GSX-DC

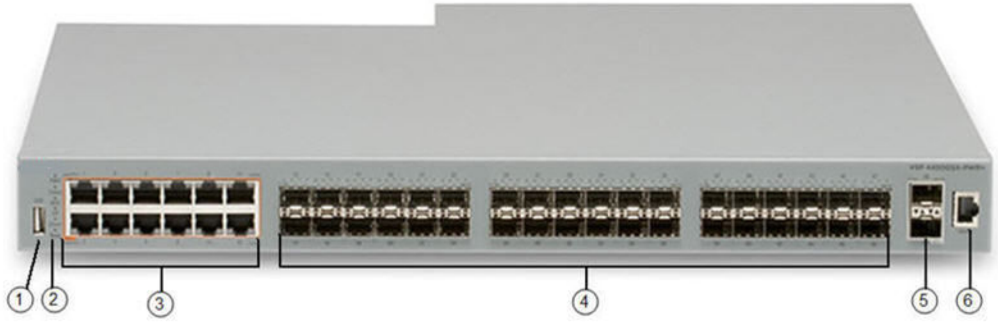


Figure 14: VSP 4450GSX-DC

1. VSP 4000 USB port.
2. Switch LEDs for system power (PWR), switch status (Status), and redundant power supply (RPS).
3. 12 10/100/1000 Mbps RJ-45 ports. LEDs indicating port activity are above the ports.

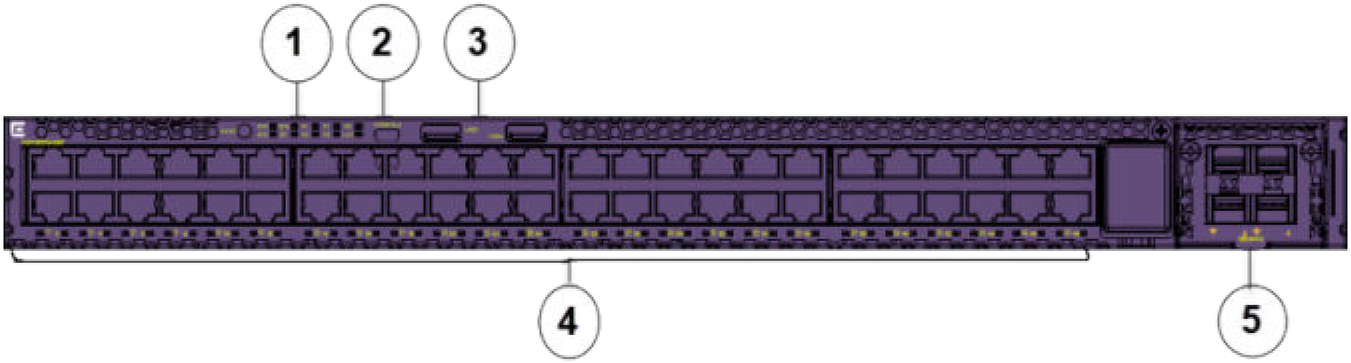
4. 36 100/1000 Mbps SPF ports.
5. Two SFP+ slots. Supports 1G SFPs and 10G SFP+s.
6. Console Port.

VSP 4900 Series

The following diagrams illustrate the components on the front panels of the VSP 4900 switches.

VSP4900-48P

The following diagram illustrates the components of the front panel of the VSP4900-48P switch. Slot 1 is used for the 48 fixed ports and slot 2 is used for Versatile Interface Module (VIM) ports, if a VIM is installed in the VIM slot.



1. Mode button for port LED control. Port LED mode indicators (SYS, SPD). Switch LEDs for system power (P1, P2) and fans (F1, F2, F3). System Locator LED (LOC).

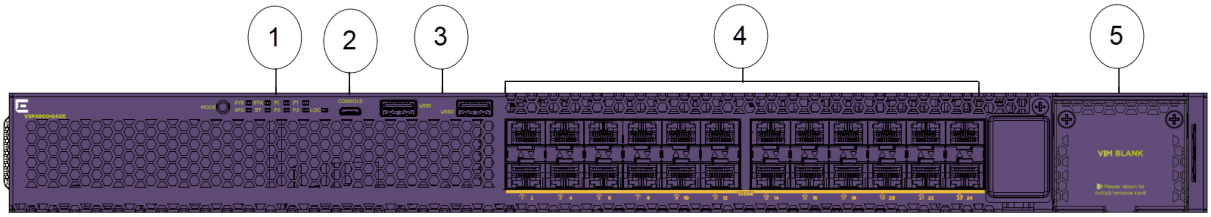
   Note:

   Note: STK and BT port LED mode indicators are not supported.
2. One USB micro B console port. An alternative RJ-45 console port is provided on the back panel (not shown).
3. Two USB ports, for removable storage.
4. 48 10/100/1000 Mbps RJ-45 Ethernet ports that provide 802.3at PoE+. LEDs that indicate the port activity and statuses are below the ports.
5. VIM slot (shown with VIM installed). Port numbering depends on the type of VIM installed in the slot. For more information about VIM modules, see VSP 4900 Series Switches: Hardware Installation Guide.

The back panel (not shown) includes an RJ-45 out of band (OOB) management port, an RJ-45 console port, and hot-swappable power supply and fan units.

VSP4900-24XE

The following diagram illustrates the components on the front panel of the VSP4900-24XE switch. Slot 1 is used for the 24 fixed ports and slot 2 is used for Versatile Interface Module (VIM) ports, if a VIM is installed in the VIM slot.

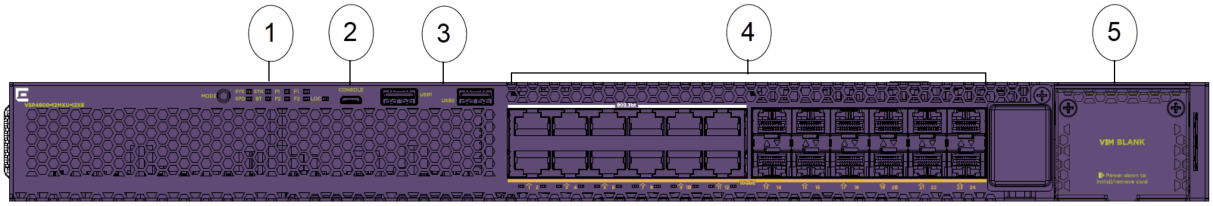


1. Mode button for port LED control. Port LED mode indicators (SYS, SPD, STK and BT). Switch LEDs for system power (P1, P2) and fans (F1, F2, F3). System Locator LED (LOC).
2. One USB micro B console port. An alternative RJ-45 console port is provided on the back panel (not shown).
3. Two USB ports, for removable storage.
4. 24 1/10 Gbps ports. LEDs that indicate the port activity and statuses are below the ports.
5. VIM slot. Port numbering depends on the type of VIM installed in the slot. For more information about VIM modules, see VSP 4900 Series Switches: Hardware Installation Guide.

The back panel (not shown) includes an RJ-45 out of band (OOB) management port, an RJ-45 console port, Solid State Drive (SSD) slot, and hot-swappable power supply and fan units.

VSP4900-12MXU-12XE

The following diagram illustrates the components on the front panel of the VSP4900-12MXU-12XE switch. Slot 1 is used for the 24 fixed ports and slot 2 is used for Versatile Interface Module (VIM) ports, if a VIM is installed in the VIM slot.

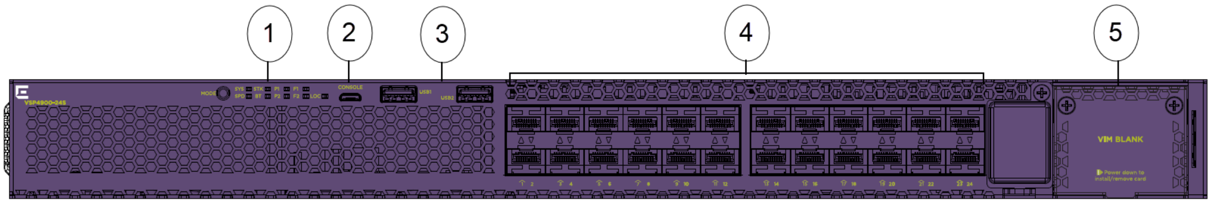


1. Mode button for port LED control. Port LED mode indicators (SYS, SPD, STK and BT). Switch LEDs for system power (P1, P2) and fans (F1, F2, F3). System Locator LED (LOC).
2. One USB micro B console port. An alternative RJ-45 console port is provided on the back panel (not shown).
3. Two USB ports, for removable storage.
4. Ports 1 to 12 are 100 Mbps and 1/2.5/5/10 Gbps RJ-45 ports that provide PoE (60W) and ports 13-24 are 1/10 Gbps ports. LEDs that indicate the port activity and statuses are below the ports.
5. VIM slot. Port numbering depends on the type of VIM installed in the slot. For more information about VIM modules, see VSP 4900 Series Switches: Hardware Installation Guide.

The back panel (not shown) includes an RJ-45 out of band (OOB) management port, an RJ-45 console port, SSD slot, and hot-swappable power supply and fan units.

VSP4900-24S

The following diagram illustrates the components on the front panel of the VSP4900-24S switch. Slot 1 is used for the 24 fixed ports and slot 2 is used for Versatile Interface Module (VIM) ports, if a VIM is installed in the VIM slot.



1. Mode button for port LED control. Port LED mode indicators (SYS, SPD, STK and BT). Switch LEDs for system power (P1, P2) and fans (F1, F2, F3). System Locator LED (LOC).
2. One USB micro B console port. An alternative RJ-45 console port is provided on the back panel (not shown).
3. Two USB ports, for removable storage.
4. 24 1 Gbps ports. LEDs that indicate the port activity and statuses are below the ports.
5. VIM slot. Port numbering depends on the type of VIM installed in the slot. For more information about VIM modules, see VSP 4900 Series Switches: Hardware Installation Guide.

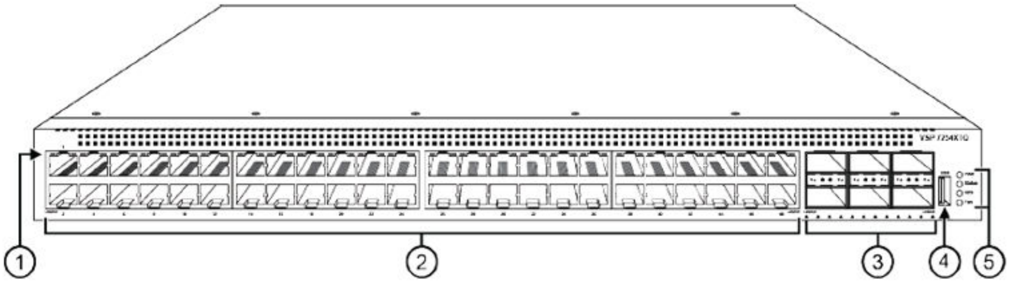
The back panel (not shown) includes an RJ-45 out of band (OOB) management port, an RJ-45 console port, and hot-swappable power supply and fan units.

VSP 7200 Series

The following figure illustrates the front view of the VSP 7200 Series switch.

When looking at the front of the switch:

- Slot 1 is the grouping of the 48 10 Gbps ports on the left.
- Slot 2 is the grouping of the 6 40 Gbps ports on 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 7400 Series

The following diagrams illustrate the components on the front panels of the switches. For more information on hardware, see VSP 7400 Series Switches: Hardware Installation Guide.

VSP 7432CQ

The following figure illustrates the components on the front panel of the VSP 7432CQ. Slot 1 is used for all of the ports.

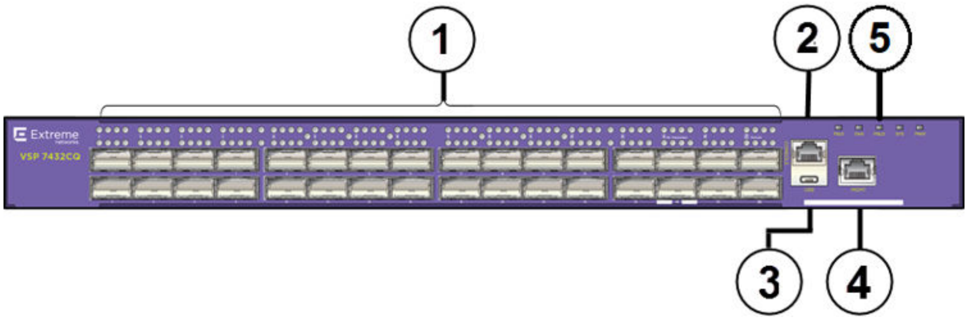


Figure 15: VSP 7432CQ

1. 32 100-Gigabit QSFP28/QSFP+ ports each with 4 LEDs — the top row of LEDs is for the top port and the lower row of LEDs is for the lower port.
2. RJ-45 console port.
3. USB port.
4. OOB Management port — LinkSpeed LED on the left and Activity LED on the right.
5. LEDs for system power, power supply units (PSU1 and PSU2), fan modules, and system.

The VSP 7432CQ supports two internal Extreme Integrated Application Hosting (IAH) ports labeled as Insight ports, 1/s1 and 1/s2, used by IAH virtual machines. For conceptual information and configuration instructions to use internal IAH ports, see Configuring User Interfaces and Operating Systems for VOSS.

VSP 7400-48Y

The following figure illustrates the components on the front panel of the VSP 7400-48Y. Slot 1 is used for all of the ports.

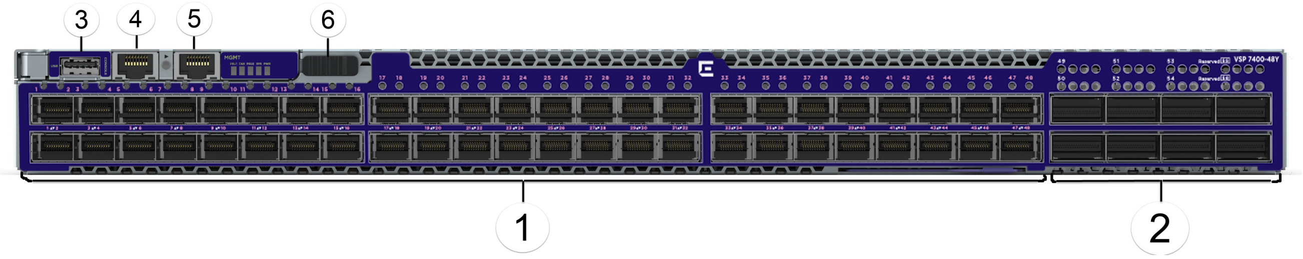


Figure 16: VSP 7400-48Y

1. 48 25-Gigabit SFP28 ports.
2. 8 100-Gigabit QSFP28/QSFP+ ports each with 4 LEDs.
3. USB port.
4. RJ-45 console port.
5. OOB Management RJ-45 port — A single LinkSpeed and Activity LED on the left.

   LEDs for system power, power supply units (PSU1 and PSU2), fan modules, and system are to the right of the management port.
6. Management Set sliding button.

The VSP 7400-48Y supports one internal IAH port, 1/s1, used by IAH virtual machines. For conceptual information and configuration instructions to use internal IAH ports, see Configuring User Interfaces and Operating Systems for VOSS.

VSP 8000 Series

The following diagrams illustrate the components on the front panels of the switches. For more information on hardware, see Installing the Virtual Services Platform 8000 Series.

VSP 8200 Series

The following figure illustrates the front view of the VSP 8284XSQ switch. There are 42 ports in Slot 1 on top, and 42 ports in Slot 2 on the bottom.

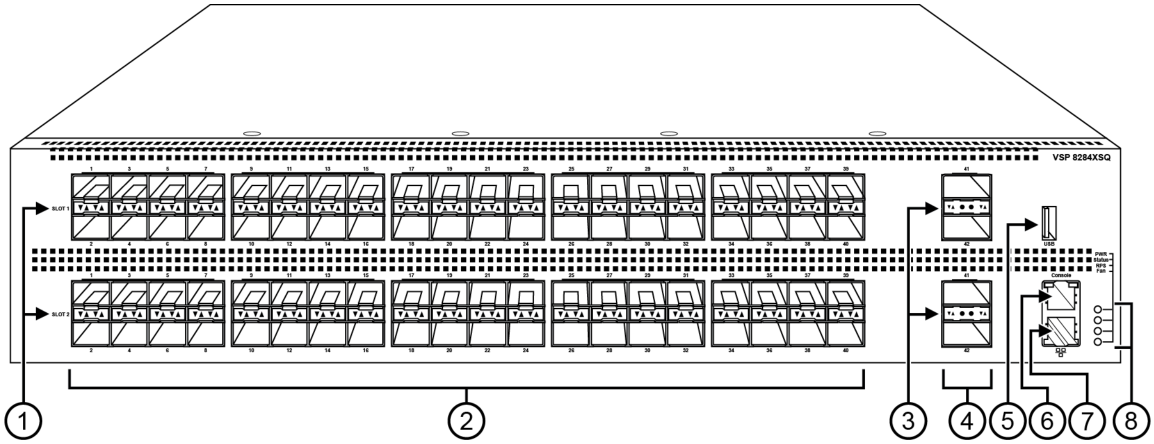


Figure 17: VSP 8284XSQ front view

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.
2. 80 SFP+ ports that support 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).

VSP 8400 Series Series

The following figure illustrates the front view of the VSP 8400 Series switch.

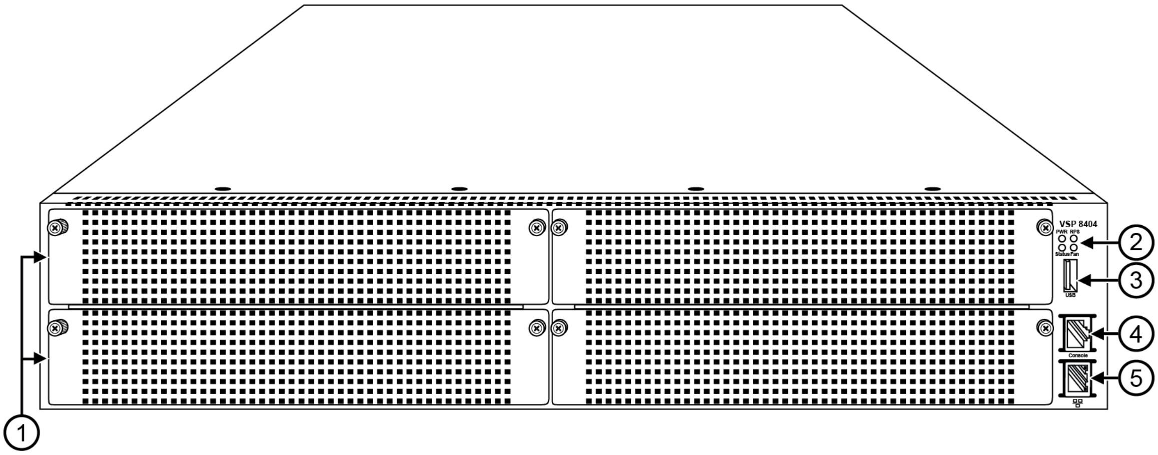


Figure 18: VSP 8404 front view

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 Virtual Services Platform 8000 Series.

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

VSP 8600 Series

The VSP 8608 chassis provides eight slots for I/O and control (IOC) modules and three slots for switch fabric (SF) modules in a 7U vertically oriented configuration.

The following figure illustrates the front view of the VSP 8600 Series switch.

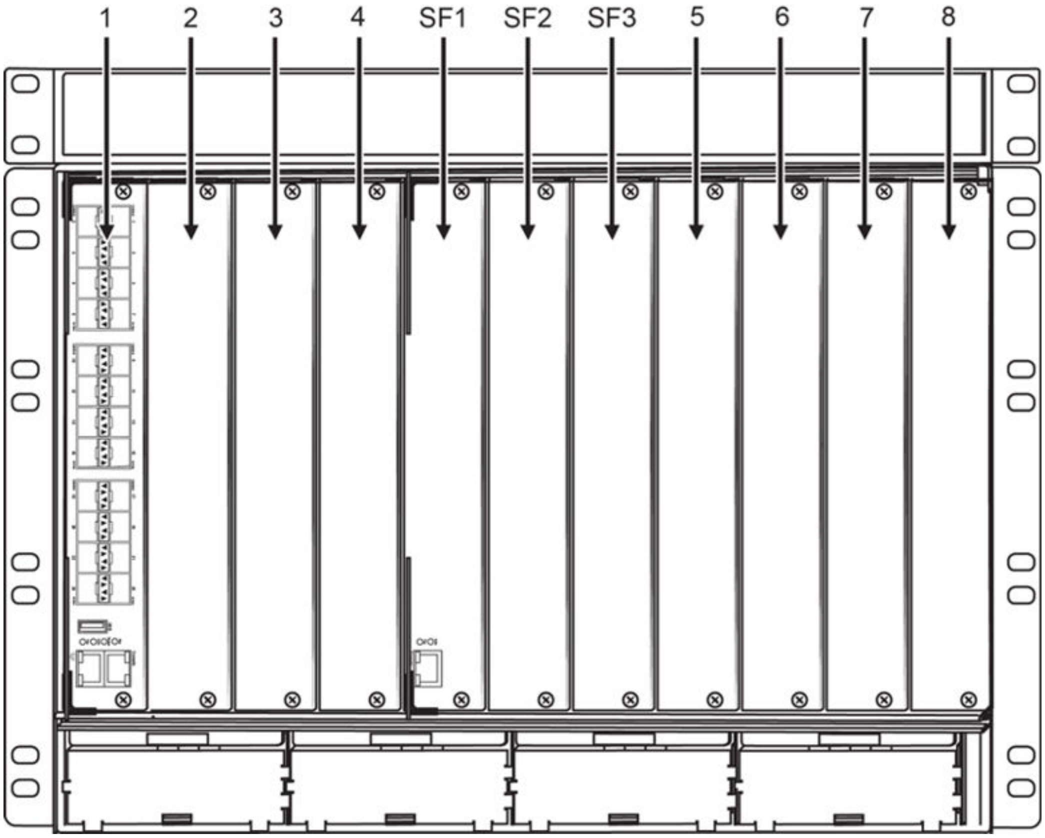


Figure 19: VSP 8608 front view

From left-to-right, slots 1 through 4 are designated for I/O and control (IOC) modules, followed by slots SF1 through SF3 for switch fabric modules, and then slots 5 through 8 for IOC modules.

The switch supports different I/O and control (IOC) module types. Port numbering depends on the type of IOC module installed in the slot. The front panel on each IOC contains an RJ–45 console port, OOB Ethernet management port, USB port, and status LED indicators. For more information about IOC modules, see Installing the Virtual Services Platform 8600.

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.

VSP 4000 Series and XA1400 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 and XA1400 Series use one slot.

VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8000 Series , and VSP 8600 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 4900 Series.

The slot numbers are 1-2 for the VSP 7200 Series.

The slot number is 1 for the VSP 7400 Series.

The slot numbers are 1-2 for the VSP 8200 Series.

The slot numbers are 1-4 for VSP 8400 Series.

The slot numbers are 1–8 for VSP 8600 Series.

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
------------------------------------------------------------------------------------------
1/1/1    192   40GbCR4BoC-Channel true  false    1950  00:c0:ff:8b:50:00 up     up
1/1/2    193   40GbCR4BoC-Channel true  false    1950  00:c0:ff:8b:50:01 down   down
1/1/3    194   40GbCR4BoC-Channel true  false    1950  00:c0:ff:8b:50:02 down   down
1/1/4    195   40GbCR4BoC-Channel true  false    1950  00:c0:ff:8b:50:03 down   down
1/2      196   100GbNone          true  false    1950  00:c0:ff:8b:50:04 down   down
1/3      200   100GbNone          true  false    1950  00:c0:ff:8b:50:08 down   down
```

```
1/4      204   100GbNone          true  false    1950  00:c0:ff:8b:50:0c down   down
1/5      208   100GbNone          true  false    1950  00:c0:ff:8b:50:10 down   down
1/6      212   100GbNone          true  false    1950  00:c0:ff:8b:50:14 down   down
1/7      216   100GbNone          true  false    1950  00:c0:ff:8b:50:18 down   down
1/8      220   100GbNone          true  false    1950  00:c0:ff:8b:50:1c down   down
1/9      224   100GbNone          true  false    1950  00:c0:ff:8b:50:20 down   down
1/10     228   100GbNone          true  false    1950  00:c0:ff:8b:50:24 down   down
1/11     232   100GbNone          true  false    1950  00:c0:ff:8b:50:28 down   down
1/12/1   236   100GbNone-Channel  true  false    1950  00:c0:ff:8b:50:2c down   down
1/12/2   237   100GbNone-Channel  true  false    1950  00:c0:ff:8b:50:2d down   down
1/12/3   238   100GbNone-Channel  true  false    1950  00:c0:ff:8b:50:2e down   down
1/12/4   239   100GbNone-Channel  true  false    1950  00:c0:ff:8b:50:2f down   down
1/13     240   100GbNone          true  false    1950  00:c0:ff:8b:50:30 down   down
1/14     244   100GbNone          true  false    1950  00:c0:ff:8b:50:34 down   down
1/15     248   100GbNone          true  false    1950  00:c0:ff:8b:50:38 down   down
1/16     252   100GbNone          true  false    1950  00:c0:ff:8b:50:3c down   down
1/17     256   100GbNone          true  false    1950  00:c0:ff:8b:50:40 down   down
1/18     260   100GbNone          true  false    1950  00:c0:ff:8b:50:44 down   down
1/19     264   100GbNone          true  false    1950  00:c0:ff:8b:50:48 down   down
1/20     268   100GbNone          true  false    1950  00:c0:ff:8b:50:4c down   down
1/21     272   100GbNone          true  false    1950  00:c0:ff:8b:50:50 down   down
1/22     276   100GbNone          true  false    1950  00:c0:ff:8b:50:54 down   down
1/23     280   100GbNone          true  false    1950  00:c0:ff:8b:50:58 down   down
1/24     284   100GbNone          true  false    1950  00:c0:ff:8b:50:5c down   down
1/25     288   100GbCR4           true  false    1950  00:c0:ff:8b:50:60 down   down
1/26     292   100GbCR4           true  false    1950  00:c0:ff:8b:50:64 down   down
1/27     296   100GbNone          true  false    1950  00:c0:ff:8b:50:68 down   down
1/28     300   100GbNone          true  false    1950  00:c0:ff:8b:50:6c down   down
1/29     301   100GbNone          true  false    1950  00:c0:ff:8b:50:6d down   down
1/30     305   100GbNone          true  false    1950  00:c0:ff:8b:50:71 down   down
1/31     309   100GbNone          true  false    1950  00:c0:ff:8b:50:75 down   down
1/32     313   100GbNone          true  false    1950  00:c0:ff:8b:50:79 down   down
1/s1     320   10GbInsight        true  false    1950  00:c0:ff:8b:50:7d down   down
1/s2     321   10GbInsight        true  false    1950  00:c0:ff:8b:50:7e down   down
```

Note:

1/s1 and 1/s2 are ports used by Extreme Integrated Application Hosting virtual machines only.

VLAN interface index

The interface index of a VLAN is computed using the following formula:

Because the default VLAN always uses an MGID value of 1, its interface index is always 2049.

ifIndex = 2048 + VLAN multicast group ID (MGID)

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
XA1400 Series	1,024	First 8	remaining 1,016
VSP 4000 Series	256	First 128	remaining 128
VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, and VSP 8000 Series	1,024	First 256	remaining 768
VSP 8600 Series	4,096	First 1,024	remaining 3,072

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 22: 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

Table 59: Supported IEEE Standards

IEEE standard	Description
802.1AB	LLDP
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 and 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 Network Access Control (NAC)
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Eletrotechnical Commission (IEC) 8802-3
802.3ab	1000 Mbps Operation, implemented as 1000BASE-T Copper
802.1AE	MAC Security

Table continues…

IEEE standard	Description
802.3ae	10 Gbps Operation, implemented as 10GBASE-X SFP+
802.3af 802.3at	Power over Ethernet (PoE)
802.3az	Energy Efficient Ethernet (EEE)
802.3ba	40 Gbps and 100 Gbps Operation, implemented as 40GBASE-QSFP+ and 100GBASE-QSFP28
802.3x	Full Duplex & Flow Control
802.3z	1000 Mbps Operation, implemented as 1000BASE-X SFP
ANSI/TIA-1057	LLDP-MED

Supported RFCs

The following table and sections list the RFCs that the switch supports.

Table 60: 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 815	IP Datagram Reassembly Algorithm
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

Table continues…

Request for comment	Description
RFC 1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC 1058	RIPv1 Protocol
RFC 1112	Host Extensions for IP Multicasting (IGMPv1)
RFC 1122	Requirements for Internet Hosts
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
RFC 1253	OSPF MIB
RFC 1256	ICMP Router Discovery
RFC 1258 ✱ **Note:** Exception: rlogin is only supported on VSP 8600 Series.	IPv6 Rlogin server
RFC 1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC 1323	TCP Timestamp (The switch is only compliant if the TCP timestamp is enabled.)
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 2132	DHCP Options and BOOTP Vendor Extensions
RFC 2138	RADIUS Authentication
RFC 2139	RADIUS Accounting
RFC 2178	OSPF MD5 cryptographic authentication / OSPFv2

Table continues…

Request for comment	Description
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)
RFC 2408	Internet Security Associations and Key Management Protocol (ISAKMP)
RFC 2453	RIPv2 Protocol
RFC 2460	IPv6 base stack
RFC 2462	IPv6 Stateless Address Autoconfiguration
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 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Services
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 2737	Entity MIB (Version 2)
RFC 2819	RMON
RFC 2865	RADIUS
RFC 2874	DNS Extensions for IPv6
RFC 2918	Route Refresh Capability for BGP-4

Table continues…

Request for comment	Description
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 3484	Default Address Selection for IPv6
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 3580	IEEE 802.1X Remote Authentication Dial In User Service
RFC 3587	IPv6 Global Unicast Address Format
RFC 3596	DNS Extensions for IPv6
RFC 3621	Power Ethernet MIB
RFC 3748	Extensible Authentication Protocol
RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 3825	Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information
RFC 3879	Deprecating Site Local Addresses
RFC 3986	Uniform Resource Identifiers (URI)
RFC 4007	IPv6 Scoped Address Architecture
RFC 4022	MIB for TCP
RFC 4113	MIB for UDP
RFC 4193	Unique Local IPv6 Unicast Address
RFC 4213	IPv6 configured tunnel
RFC 4250–RFC 4256	SSH server and client support
RFC 4291	IPv6 Addressing Architecture
RFC 4293	MIB for IP
RFC 4301	Security Architecture for IPv6
RFC 4302	IP Authentication Header (AH)

Table continues…

Request for comment	Description
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 4649	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
RFC 4675	Egress VLAN
RFC 4760	Multiprotocol Extensions for BGP-4
RFC 4835	Cryptographic algorithm implementation for ESP and AH
RFC 4861	IPv6 Neighbor discovery
RFC 4862	IPv6 stateless address autoconfiguration
RFC 4893	BGP Support for Four-octet AS Number Space
RFC 5095	Deprecation of Type 0 Routing headers in IPv6
RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
RFC 5187	OSPFv3 Graceful Restart (helper-mode only)
RFC 5242	The Syslog Protocol
RFC 5321	Simple Mail Transfer Protocol
RFC 5340	OSPF for IPv6
RFC 5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
RFC 5997	Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol
RFC 6105	IPv6 Router Advertisement Guard
RFC 6329	IS-IS Extensions supporting Shortest Path Bridging

Table continues…

Request for comment	Description
RFC 7047	The Open vSwitch Database Management Protocol
RFC 7348	Virtual Extensible LAN (VXLAN)
RFC 7610	DHCPv6 Shield

Quality of service

Table 61: 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 62: 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)

Table continues…

Request for comment	Description
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2616	IPv6 HTTP server
RFC2819	Remote Network Monitoring Management Information Base
RFC 3411	Architecture for describing SNMP Management Frameworks
RFC4292	IP Forwarding Table MIB

MIBs

Table 63: 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

Table continues…

Request for comment	Description
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)
RFC4292	IP Forwarding Table MIB
RFC4363	Bridges with Traffic MIB
RFC4673	RADIUS Dynamic Authorization Server MIB

Standard MIBs

The following table details the standard MIBs that the switch supports.

Table 64: 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

Table continues…

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
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

Table continues…

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934	rfc2934.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control protocol (TCP)	RFC4022	rfc4022.mib
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	q-bridge.mib
LLDP-EXT-MED-MIB — LLDP-MED	ANSI/TIA-1057	lldpExtMed.mib

Proprietary MIBs

The following table details the proprietary MIBs that the switch supports.

Table 65: Proprietary MIBs

Proprietary MIB name	File name
Extreme Networks Energy Saver MIB	bayStackNes.mib
Extreme Networks Link-state tracking (LST) MIB	bayStackLinkStateTracking.mib
Extreme Networks IGMP MIB	rfc_igmp.mib
Extreme Networks IP Multicast MIB	ipmroute_rcc.mib
Extreme Networks MIB definitions	wf_com.mib
Extreme Networks PIM MIB	pim-rcc.mib

Table continues…

Proprietary MIB name	File name
Extreme Networks RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Extreme Networks 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 ✱ **Note:** The MACsec tables, namely, rcMACSecCATable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	rapid_city.mib
SynOptics Root MIB	synro.mib

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 the 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).

High Availability-CPU (HA-CPU)

The HA-CPU feature activates two CPUs simultaneously in master or standby role so that, if a failure occurs, one of the CPUs can take over the operations of the other.

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.