ExtremeSwitching™

Quick Start Configuration for VOSS

Release 8.1 (VOSS)
9035869 Rev AA
October 2019

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, please 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: www.extremenetworks.com/support/policies/software-licensing

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 document provides instructions to perform basic configuration of the chassis and software.

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: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

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. 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.

Table continues…

Convention	Description
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 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

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, 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: 1-800-998-2408 (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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing 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 with your information (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. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have 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 especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please 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.

VSP 4900 Series

VSP 4900-48P is a new hardware model that is ideal for small sites where there is a need to extend Fabric Connect technology across a wide area, a metro area, or to a campus edge. In these scenarios, the VSP 4900-48P can help segment traffic for regulatory or security reasons or to support multiple entities or tenants.

The VSP 4900-48P provides 48 fixed MACsec-capable 10/100/1000 Mbps RJ-45 Ethernet ports with 802.3at PoE+ (30W).

In addition to the 48 fixed copper-based ports, the VSP 4900-48P provides one Versatile Interface Module (VIM) slot. Any one of the following VIMs can be installed in the VIM slot to provide flexible linkage to other switches or devices over a range of media.

- VIM5-4X: Four SFP+ ports of 1/10 Gbps.
- VIM5-4XE: Four SFP+ ports of 10 Gbps, supporting MACSec and LRM.
- VIM5-2Y: Two SFP28 ports of 10/25 Gbps.
- VIM5-4YE: Four SFP28 ports of 10/25 Gbps. Only the first two ports are supported.
- VIM5-2Q: Two QSFP ports of 10 Gbps (with channelization) or 40 Gbps. Only the first port is supported.

The VSP 4900-48P also provides a choice of console interface ports (one micro USB and one RJ-45), one RJ-45 out of band (OOB) management port, two USB ports for removable storage, and hot-swappable, redundant power supplies and fans.

For more information, see:

- System Connections on page 14
- Connect a Terminal on page 22

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 appear on your hardware, it is not supported.

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

Chapter 3: Fundamentals

Perform provisioning after hardware installation.

This document includes the minimum, but essential, configuration steps to:

- provide a default, starting point configuration
- establish a management interface
- establish basic security on the node

For more information about hardware specifications and installation procedures, see the following documents:

- Installing the Virtual Services Platform 4450GSX-PWR+
- Installing the Virtual Services Platform 4850GTS Series
- Installing the Virtual Services Platform 4450GTX-HT-PWR+
- VSP 4900 Series Switches: Hardware Installation Guide
- Installing the Virtual Services Platform 7200 Series
- VSP 7400 Series Switches: Hardware Installation Guide
- Installing the Virtual Services Platform 8000 Series
- Installing the Virtual Services Platform 8600
- XA1400 Series Switches: Hardware Installation Guide

For more information about how to configure security, see Configuring Security for VOSS.

Important operational note for VSP 4000 Series switches

This section provides information to take into consideration to prevent system operation failure.

Operational consideration for USB Flash Drive on factory supplied and converted VSP 4000 Series switches
Warning: 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. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 Series switch is

Operational consideration for USB Flash Drive on factory supplied and converted VSP 4000 Series switches
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.

ERS 4850 and VSP 4000 quick conversion

Note:

ERS 4850 and VSP 4000 conversion kit (part number EC4810003–3.0) has reached End-Of-Sale; however, it is still supported for anyone who has purchased it.

You can convert an ERS 4850 switch to a VSP 4000 switch, if there is a network requirement.

USB considerations for factory supplied and converted VSP 4000 switches
Warning: The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

On a converted VSP 4000 switch, you can also use the CLI to perform a conversion back to the ERS 4850.

For the conversion to be successful, you must ensure that you have satisfied the hardware and software criteria on the system being converted.

spbm-config-mode boot flag

Shortest Path Bridging (SPB) and Protocol Independent Multicast (PIM) cannot interoperate with each other on the switch at the same time. To ensure that SPB and PIM stay mutually exclusive, 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 information about verifying boot flags, see Verifying boot configuration flags on page 62. For more information about this boot flag and Simplified vIST, see Configuring IP Multicast Routing Protocols for VOSS.

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.

System logon

After the platform boot sequence is complete, a logon prompt appears. The following table shows the default values for logon and password for console and Telnet sessions.

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.

Table 3: Access levels and default logon values

Access level	Description	Default logon	Default password
Read-only	Permits view-only configuration and status information. Is equivalent to Simple Network Management Protocol (SNMP) read-only community access.	ro	ro
Layer 1 read/write	View most switch configuration and status information and change physical port settings.	l1	l1
Layer 2 read/write	View and change configuration and status information for Layer 2 (bridging and switching) functions.	l2	l2
Layer 3 read/write	View and change configuration and status information for Layer 2 and Layer 3 (routing) functions.	l3	l3
Read/write	View and change configuration and status information across the switch. You cannot 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, including CLI and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

Secure and nonsecure protocols

The following table describes the secure and nonsecure protocols that the switch supports.

Table 4: Secure and nonsecure protocols for IPv4 and IPv6

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
FTP and Trivial FTP	Disabled	Secure Copy (SCP) and Secure File Transfer Protocol (SFTP)	Disabled
Note: File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.			
Telnet	Disabled	Secure Shell version 2 (SSHv2)	Disabled
SNMPv1, SNMPv2	Enabled	SNMPv3	Enabled
Rlogin	Disabled	SSHv2	Disabled
HTTP	Disabled	HTTPS **Important:** Take the appropriate security precautions within the network if you use HTTP. You must use the **`web-server enable`** command in CLI before you can access EDM.	Enabled

Password encryption

The platform stores passwords in encrypted format and not in the configuration file.

Important:

For security reasons, configure the passwords to values other than the factory defaults.

Enterprise Device Manager

The switch includes Enterprise Device Manager (EDM), an embedded graphical user interface (GUI) that you can use to manage and monitor the platform through web-based access without additional installations.

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

Enterprise Device Manager access

To access EDM, enter one of the following addresses in your web browser:

- http://<A.B.C.D>
- https://<A.B.C.D>

Where <A.B.C.D> is the device IP address.

Ensure you use a supported browser version. For more information about supported browsers, see Configuring User Interfaces and Operating Systems for VOSS.

Important:

- You must enable the Web server from CLI to enable HTTP access to the EDM. If you want HTTP access to the device, you must also disable the web server secure-only option. The web server secure-only option, allowing for HTTPS access to the device, is enabled by default. Take the appropriate security precautions within the network if you use HTTP.
- EDM access is available to read-write users only.

If you experience any issues while connecting to the EDM, check the proxy settings. Proxy settings may affect EDM connectivity to the switch. Clear the browser cache and do not use proxy when connecting to the device. This should resolve the issue.

Default user name and password

The following table contains the default user name and password that you can use to log on to the switch using EDM. For more information about changing the passwords, see Configuring Security for VOSS.

Table 5: EDM default username and password

Username	Password
admin	password

Important:

The default passwords and community strings are documented and well known. It is strongly recommended that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see Configuring Security for VOSS.

Device Physical View

After you access EDM, the system displays a real-time physical view of the front panel of the device. From the front panel view, you can view fault, configuration, and performance information for the device or a single port. You can open this tab by clicking the Device Physical View tab above the device view.

You can use the device view to determine the operating status of the various ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects. In the device view, you can select a port or the entire chassis. To select an object, click the object. EDM outlines the selected object in yellow, indicating your selection.

The conventions on the device view are similar to the actual device appearance. The port LEDs and the ports are color-coded to provide status. Green indicates the module or port is up and running, red indicates the module or port is disabled, dark pink indicates a protocol is down, and amber indicates an enabled port that is not connected to anything. For information about LED behavior, see your hardware documentation.

EDM Window

The following list identifies the different sections of the EDM window:

- Navigation pane—Located on the left side of the window, the navigation pane displays all the available command tabs in a tree format. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.
- Content pane—Located on the right side of the window, the content pane displays the tabs and dialog boxes where you can view or configure parameters on the switch.
- Menu bar—Located at the top of the content pane, the menu bar shows the most recently accessed primary tabs and their respective secondary tabs.
- Toolbar—Located just below the menu bar, the toolbar provides quick access to the most common operational commands such as Apply, Refresh, and Help.

The following figure shows an example of the Device Physical View tab within the EDM window.

Note:

The Device Physical View tab on your hardware can appear differently than the following example.

Figure 1: EDM window

IP address for the management port

At startup, the system loads the runtime configuration file, which is stored in the internal flash of the CPU. If the file is present, the system assigns the IP address for the management port from that file.

You can configure an IP address for the management port if one is not in the configuration file. For more information, see Configuring an IP address for the management port on page 30. This procedure only applies to hardware with a dedicated, physical management interface.

Static routes

A static route is a route to a destination IP address that you manually create.

The Layer 3 redundancy feature supports the creation of static routes to enhance network stability. Use the local next hop option to configure a static route with or without local next hop.

You can configure static routes with a next hop that is not directly connected, but that hop must be reachable. Otherwise, the static route is not enabled.

Layer 3 redundancy supports only address resolution protocol (ARP) and static route. Static ARP must configure the nonlocal next-hop of static routes. No other dynamic routing protocols provide nonlocal next-hop.

You can use a default static route to specify a route to all networks for which no explicit routes exist in the forwarding information base or the routing table. This route has a prefix length of zero (RFC1812). You can configure the switch with a route through the IP static routing table.

To create a default static route, you must configure the destination address and subnet mask to 0.0.0.0.

Static route tables

A router uses the system routing table to make forwarding decisions. In the static route table, you can change static routes directly. Although the two tables are separate, the static route table manager entries are automatically reflected in the system routing table if the next-hop address in the static route is reachable, and if the static route is enabled.

The system routing table displays only active static routes with a best preference. A static route is active only if the route is enabled and the next-hop address is reachable (for example, if a valid ARP entry exists for the next hop).

You can enter multiple routes (for example, multiple default routes) that have different costs, and the routing table uses the lowest cost route that is available. However, if you enter multiple next hops for the same route with the same cost, the software does not replace the existing route. If you enter the same route with the same cost and a different next-hop, the first route is used. If the first route becomes unreachable, the second route (with a different next-hop) is activated with no connectivity loss.

Static ARP entries

Static ARP entries are not supported for NLB Unicast or NLB Multicast operations.

Chapter 4: Provisioning

This section contains procedures for the initial provisioning of the switch. These procedures should always be performed when provisioning the switch.

Configuring the switch

You can use the information below to configure the switch. The examples show you how to enable the access service, change the root level prompt, configure the CLI logon banner, enable the web-server, and specify a gateway address route.

Before you begin

You must enable Global Configuration mode in CLI.

About this task

Configure the switch. You can copy and paste the configuration in the example or modify it as desired.

Example

```
boot config flags ftpd
boot config flags sshd
boot config flags telnetd
boot config flags tftpd
save config

prompt "Lab4Switch"
banner custom
banner "Welcome to Switch located in Lab 4, Blue Zone"
banner displaymotd

web-server enable
no web-server secure-only
```

The following example describes the procedure for assigning an IP address to a VLAN interface.

```
interface vlan <vid>
ip address  x.x.x.x 255.255.255.0
```

The following example describes the procedure for assigning an IP address to a port interface.

```
interface gigabitEthernet 1/1
brouter vlan <vid> subnet x.x.x.x 255.255.255.0
```

Connect a Terminal

Before you begin

- To use the console port, you need the following equipment:
  - A terminal or TeleTypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software
  - A specific cable with an RJ–45 or USB connector for the console port on the switch. The other end of the cable must use a connector appropriate to the serial port on your computer or terminal.
- You must shield the cable that connects to the console port to comply with emissions regulations and requirements.

Note:

If you are using the VSP 4900-48P USB console port with a terminal running Windows 10, you must install the CP210x USB to UART Bridge Virtual COM Port (VCP) driver from Silicon Labs before you make the connection.

About this task

Connect a terminal to the serial console interface to monitor and configure the system directly.

Procedure

1. Configure the terminal protocol as follows:
   - 9600 baud or 115200 baud depending on the hardware platform.
   - 8 data bits
   - 1 stop bit
   - No parity
   - No flow control
2. Connect the RJ–45 or USB cable to the console port on the switch.
3. Connect the other end of the cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Log on to the switch.

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.

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.

If you enable enhanced secure mode with the **boot config flags enhancedsecure-mode** command, you enable new access levels, along with stronger password complexity, length, and minimum change intervals. For more information on system access fundamentals and configuration, see Administering VOSS.

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.

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. Re-enter the new password.
6. Configure password options:

   ```
   password [access-level WORD<2-8>] [aging-time day <1-365>] [default-
   lockout-time <60-65000>] [lockout WORD<0-46> time <60-65000>] [min-
   passwd-len <10-20>] [password-history <3-32>]
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal
```

Change a password:

```
Switch:1(config)# cli password rwa read-write-all
```

Enter the old password: ***

Enter the new password: ***

Re-enter the new password: ***

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

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

Variable definitions

Use the data in the following table to use the `cli password` command.

Table 6: Variable definitions

Variable	Value
layer1|layer2|layer3|read-only|read-write|read-write-all	Changes the password for the specific access level.
WORD<1–20>	Specifies the user logon name.

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

Table 7: Variable definitions

Variable	Value
access-level *WORD<2–8>*	Permits or blocks this access level. The available access level values are as follows: • layer1 • layer2 • layer3 • read-only • read-write • read-write-all
aging-time day *<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 IPv4 or IPv6 address. • *<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.

Table continues…

Variable	Value
password-history <*3-32*>	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default is 3. To configure this option to the default value, use the default operator with the command.

Configuring system identification

Configure system identification to specify the system name, contact person, and location of the switch.

Procedure

1. Log on as rwa.
2. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

3. Change the system name:

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

4. Configure the system contact:

   ```
   snmp-server contact WORD<0-255>
   ```

5. Configure the system location:

   ```
   snmp-server location WORD<0-255>
   ```

Example

Change the system name, configure the system contact, and configure the system location:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#sys name Floor3Lab2
Floor3Lab2:1(config)#snmp-server contact http://companyname.com
Floor3Lab2:1(config)#snmp-server location "12 Street, City, State, Zip"
```

Variable definitions

Use the data in the following table to use the system-level commands.

Table 8: Variable definitions

Variable	Value
contact *WORD<0–255>*	Identifies the contact person who manages the node. To include blank spaces in the contact, use quotation marks (") around the text. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
location *WORD<0–255>*	Identifies the physical location of the node. To include blank spaces in the location, use quotation marks (") around the text. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
name *WORD<0–255>*	Configures the system or root level prompt name for the switch. *WORD<0–255>* is an ASCII string from 1–255 characters (for example, LabSC7 or Closet4).

Configuring the CLI Banner

Configure the logon banner to display a message to users before authentication and configure a system login message-of-the-day in the form of a text banner that appears after each successful logon.

About this task

You can use the custom logon banner to display company information, such as company name and contact information. For security, you can change the default logon banner of the switch, which contains specific system information, including platform type and software release.

Use the custom message-of-the-day to update users on a configuration change, a system update or maintenance schedule. For security purposes, you can also create a message-of-the-day with a warning message to users that, “Unauthorized access to the system is forbidden.”

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>
   ```

Note:

To enter multiple lines for a message, use the **banner** command before each new line of the message. To provide a string with spaces, include the text in quotation marks.

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

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

   Note:

   To enter multiple lines for a message, use the **banner motd** command before each new line of the message. To provide a string with spaces, include the text in quotation marks.

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

   ```
   banner displaymotd
   ```

6. Save the configuration:

   ```
   save config
   ```

7. Display the banner information:

   ```
   show banner
   ```

8. Logon again to verify the configuration.

9. **(Optional)** Disable the banner:

   ```
   no banner [displaymotd][motd]
   ```

Example

Configure the custom banner to “Company, www.Companyname.com.” and configure the message of the day to “Unauthorized access to this system is forbidden. Please logout now.”

```
Switch:1> enable
Switch:1#configure terminal
Switch:1(config)# banner custom
Switch:1(config)# banner Company
Switch:1(config)# banner www.Companyname.com
Switch:1(config)# banner motd "Unauthorized access to this system is forbidden"
Switch:1(config)# banner motd "Please logout now"
Switch:1(config)#banner displaymotd
Switch:1(config)#show banner
Company
www.company.com
               defaultbanner : false
               custom banner :


                 displaymotd : true
                 custom motd :
Unauthorized access to this system is forbidden
Please logout now
```

Variable definitions

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

Variable	Value
custom	Disables the use of the default banner.
static	Activates the use of the default banner.
WORD <1–80>	Adds lines of text to the CLI logon banner.
motd *WORD<1–1516>*	Create the message of the day. To provide a string with spaces, include the text in quotation marks (“).
displaymotd	Enable the custom message of the day.

Configuring the time zone

About this task

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

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Save the changed configuration.

Example

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

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

Variable definitions

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

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

Configuring the date

About this task

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

Procedure

1. To enter User EXEC mode, log on to the switch.
2. Configure the date:

   ```
   clock set <MMddyyyyhhmmss>
   ```

3. Verify the configuration:

   ```
   show clock
   ```

Example

Configure the date and time, and then verify the configuration.

```
Switch:1>enable
Switch:1#clock set 19042014063030
Switch:1#show clock
Wed Mar 19 06:30:32 2014 EDT
```

Variable definitions

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

Table 9: Variable definitions

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

Configuring an IP address for the management port

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

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

Note:

This procedure applies only to hardware with a dedicated physical management interface. Also, not all speeds are supported on hardware platforms that support a management interface. For more information about supported interfaces and speeds, see your hardware documentation.

Before you begin

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

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface mgmtEthernet <mgmt | 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

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

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

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

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

Configuring static routes

Before you begin

- Ensure no black hole static route exists.

About this task

Configure a static route when you want to manually create a route to a destination IP address.

If a black hole route is enabled, you must first delete or disable it before you can add a regular static route to that destination.

For route scaling information and for information on the maximum number of static routes supported on your hardware platform, see Release Notes for VOSS.

Note:

It is recommended that you do not configure static routes on a DvR Leaf node unless the configuration is for reachability to a management network using a Brouter port.

Also, configuring the preference of static routes is not supported on a Leaf node.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

   ```
   enable
   configure terminal
   ```

   Optional: `router vrf WORD<1-16>`

2. Create an IP static route:

   ```
   ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> weight <1-65535>
   ```

3. Enable an IP static route:

   ```
   ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> enable
   ```

4. Use the following variable definitions table to configure other static route parameters as required.

5. View existing IP static routes for the device, or for a specific network or subnet:

   ```
   show ip route static
   ```

6. Delete a static route:

   ```
   no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D>
   ```

Example

Create an IP static route, enable a static route, and view the existing IP static routes for the device, or for a specific network or subnet.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip route 192.0.2.2 255.255.0.0 198.51.100.24 weight 20 preference 1
Switch:1(config)#ip route 192.0.2.2 255.255.0.0 198.51.100.24 enable
Switch:1(config)#show ip route static
================================================================================
                          IP Static Route - GlobalRouter
================================================================================

DEST       MASK          NEXT            NH-VRF       COST PREF LCLNHOP STATUS ENABLE
--------------------------------------------------------------------------------

192.0.2.2  255.255.255.0 198.51.100.24  GlobalRouter 20    1    TRUE    ACTIVE TRUE
```

Variable definitions

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

Table 10: Variable definitions

Variable	Value
<A.B.C.D> <A.B.C.D> <A.B.C.D>	The first and second <A.B.C.D> specify the IP address and mask for the route destination. The third <A.B.C.D> specifies the IP address of the next-hop router (the next router at which packets must arrive on this route). When you create a black hole static route, configure this parameter to 255.255.255.255 as the IP address of the router through which the specified route is accessible.
disable	Disables a route to the router or VRF.
enable	Adds a static route to the router or VRF. The no form of this command is `no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> enable`. The default form of this command is `default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> enable`.
local-next-hop enable	Enables the local next hop for this static route. The default form of this command is `default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> local-next-hop enable`. The no form of this command is `no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> local-next-hop enable`.
next-hop-vrf *<WORD 0-16>*	Specifies the next-hop VRF instance by name. After you configure the next-hop-vrf parameter, the static route is created in the local VRF, and the next-hop route is resolved in the next-hop VRF instance (next-hop-vrf). The default form of this command is `default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> next-hop-vrf <WORD 0-16>`. The no form of this command is `no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> next-hop-vrf <WORD 0-16>`.
weight *<1-65535>*	Specifies the static route cost. The default form of this command is `default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> weight`.
preference *<1-255>*	Specifies the route preference. The default form of this command is `default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> preference`.

Use the data in the following table to use the `show ip route static` command.

Table 11: Variable definitions

Variable	Value
<A.B.C.D>	Specifies the route by IP address.

Table continues…

Variable	Value
-s { <*A.B.C.D*> <*A.B.C.D*> | default}	Specifies the route by IP address and subnet mask.
vrf *WORD<0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Configuring static routes using EDM

About this task

Use static routes to force the router to make certain forwarding decisions. Create IP static routes to manually provide a path to destination IP address prefixes.

Note:

It is recommended that you do not configure static routes on a DvR Leaf node unless the configuration is for reachability to a management network using a Brouter port.

Also, configuring the preference of static routes is not supported on a Leaf node.

For route scaling information, see Release Notes for VOSS.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **IP**.
3. Click the **Static Routes** tab.
4. Click **Insert**.
5. If required, in the **OwnerVrfId** check box, select the appropriate VRF ID. By default, the VRF is the GlobalRouter VRF 0.
6. In the **Dest** field, type the IP address.
7. In the **Mask** field, type the subnet mask.
8. In the **NextHop** field, type the IP address of the router through which the specified route is accessible.
9. **(Optional)** In the **NextHopVrfId** field, select the appropriate value.
10. **(Optional)** To enable the static route, select the **Enable** check box.
11. **(Optional)** In the **Metric** field, type the metric.
12. **(Optional)** In the **Preference** field, type the route preference.
13. **(Optional)** If required, select the **LocalNextHop** check box.

    Use this option to create Layer 3 static routes.
14. Click **Insert**.

The new route appears in the **IP** dialog box, **Static Routes** tab.

Static Routes field descriptions

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

Name	Description
OwnerVrfId	Specifies the VRF ID for the static route.
Dest	Specifies the destination IP address of this route. A value of 0.0.0.0 is a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.
Mask	Indicates the mask that the system operates a logically AND function on, with the destination address, to compare the result to the Route Destination. For systems that do not support arbitrary subnet masks, an agent constructs the Route Mask by determining whether it belongs to a class A, B, or C network, and then uses one of: 255.0.0.0—Class A 255.255.0.0—Class B 255.255.255.0—Class C If the Route Destination is 0.0.0.0 (a default route) then the mask value is also 0.0.0.0.
NextHop	Specifies the IP address of the next hop of this route. In the case of a route bound to an interface which is realized through a broadcast media, the Next Hop is the IP address of the agent on that interface. When you create a black hole static route, configure this parameter to 255.255.255.255.
NextHopVrfId	Specifies the next-hop VRF ID in interVRF static route configurations. Identifies the VRF in which the ARP entry resides.
Enable	Determines whether the static route is available on the port. The default is enable. If a static route is disabled, it must be enabled before it can be added to the system routing table.
Status	Specifies the status of the route. The default is enabled.
Metric	Specifies the primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route RouteProto value. If this metric is not used, configure the value to 1. The default is 1.
IfIndex	Specifies the route index of the Next Hop. The interface index identifies the local interface through which the next hop of this route is reached.

Table continues…

Name	Description
Preference	Specifies the routing preference of the destination IP address. If more than one route can be used to forward IP traffic, the route that has the highest preference is used. The higher the number, the higher the preference.
LocalNextHop	Enables and disables LocalNextHop. If enabled, the static route becomes active only if the system has a local route to the network. If disabled, the static route becomes active if the system has a local route or a dynamic route.

Enabling remote access services

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.

About this task

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

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable the access service:

   ```
   boot config flags <ftpd|rlogind|sshd|telnetd|tftpd>
   ```

3. Repeat as necessary to activate the desired services.
4. Save the configuration.

Example

Enable the access service for Telnet:

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

Variable definitions

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

Table 12: Variable definitions

Variable	Value
ftpd	Enables the File Transfer Protocol remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
rlogind	Enables the rlogin remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
spbm-config-mode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. Use the no operator so that you can configure PIM and IGMP. The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.
sshd	Enables the Secure Shell remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
telnetd	Enables the Telnet remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
tftpd	Enables the Trivial File Transfer Protocol remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Using Telnet to log on to the device

About this task

Use Telnet to log on to the device and remotely manage the switch.

Procedure

1. From a PC or terminal, start a Telnet session:

   ```
   telnet <ipv4 or ipv6 address>
   ```

2. Enter the logon and password when prompted.

Example

```
C:\Users\jsmith>telnet 192.0.2.40
Connecting to 192.0.2.40.....
Login:rwa
Password:rwa
```

Enable the Web Management Interface

About this task

Enable the web management interface to provide management access to the switch using a web browser.

HTTP and HTTPS, and FTP support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Important:

If you want to allow HTTP access to the device, then you must disable the web server secure-only option. If you want to allow HTTPS access to the device, the web server secure-only option is enabled by default. The TFTP server supports both IPv4 and IPv6 TFTP clients.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the web server:

   ```
   web-server enable
   ```

3. To enable the secure-only option (for HTTPS access), enter:

   ```
   web-server secure-only
   ```

4. **(Optional)** To disable the secure-only option (for HTTP access), enter:

   ```
   no web-server secure-only
   ```

5. Configure the username and the access password:

   ```
   web-server password rwa WORD<1-20> WORD<1-32>
   ```

Important:

The default passwords and community strings are documented and well known. You are strongly recommended to change the default passwords and community strings immediately after you first log on.

6. Enable read-only user:

   ```
   web-server read-only-user enable
   ```

7. Save the configuration:

   ```
   save config
   ```

8. Display the web server status:

   ```
   show web-server
   ```

Example

Enable the secure-only web-server. Configure the Read-Write-All access level username to smith2 and the password to 90Go2437. Enable read-only-user for the web server. Configure the read-only-user username to jones6 and the password to G69s8672.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#web-server enable
Switch:1(config)#web-server secure-only
Switch:1(config)#web-server read-only-user enable
Switch:1(config)#web-server password ro jones6 G69s8672
Switch:1(config)#web-server password rwa smith2 90Go2437
Switch:1(config)#show web-server

Web Server Info :

        Status                    : on
        Secure-only               : enabled
        TLS-minimum-version       : tlsv12
        RO Username Status        : enabled
        RO Username               : jones6
        RO Password               : ********
        RWA Username              : smith2
        RWA Password              : ********
        Def-display-rows          : 30
        Inactivity timeout        : 900 sec
        Html help tftp source-dir :
        HttpPort                  : 80
        HttpsPort                 : 443
        NumHits                   : 0
        NumAccessChecks           : 0
        NumAccessBlocks           : 0
        NumRxErrors               : 0
        NumTxErrors               : 0
        NumSetRequest             : 0
        Minimum password length   : 8
        Last Host Access Blocked  : 0.0.0.0
        In use certificate        : Self signed
```

Variable Definitions

Use the data in the following table to use the **`web-server`** command.

Variable	Value
def-display-rows *<10-100>*	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the Web interface. To disable the web server, use the no form of this command: `no web-server [enable]`
help-tftp *<WORD/0-256>*	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/help • 192.0.2.1:/
http-port *<80-49151>*	Configures the web server HTTP port. The default port is 80.
https-port *<443-49151>*	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout*<30–65535>*	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro | rwa} *WORD<1-20> WORD<1-32>*	Configures the logon and password for the web interface, where the first *WORD<1-20>* is the new logon and the second *WORD<1-32>* is the new password.
password min-passwd-len*<1–32>*	Configures the minimum password length. By default, the minimum password length is 8 characters.
read-only-user	Enables read-only user for the web server.
secure-only	Enables secure-only access for the web server.
tls-min-ver*<tlsv10|tlsv11|tlsv12>*	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2 The default is tlsv12.

Enable the Web Server RO User

About this task

Perform this procedure to enable the web server RO user, which is disabled by default after a software upgrade.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the read-only user:

   ```
   web-server read-only-user enable
   ```

Example

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

Enable the default ro username:

```
Switch1:(config)#web-server read-only-user enable
```

Display the output of the **`show web-server command`** with the ro username enabled:

```
Switch:1(config)#show web-server
Web Server Info :

        Status                     : on
        Secure-only                : enabled
        TLS-minimum-version        : tlsv12
        RO Username Status         : enabled
        RO Username                : jones6
        RO Password                : ********
        RWA Username               : smith2
        RWA Password               : ********
        Def-display-rows           : 30
        Inactivity timeout         : 900 sec
        Html help tftp source-dir  :
        HttpPort                   : 80
        HttpsPort                  : 443
        NumHits                    : 87
        NumAccessChecks            : 4
        NumAccessBlocks            : 0
        NumRxErrors                : 73
        NumTxErrors                : 0
        NumSetRequest              : 0
        Minimum password length    : 8
        Last Host Access Blocked   : 0.0.0.0
        In use certificate         : Self signed
```

Setting the TLS protocol version

The switch by default supports version TLS 1.2 and above. You can explicitly configure TLS 1.0 and TLS 1.1 version support using CLI.

About this task

Disable the web server before changing the TLS version. By disabling the web server, other existing users with a connection to the web server are not affected from changing to a different version after you run the **`tls-min-ver`** command.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the Web server:

   ```
   no web-server enable
   ```

3. Set the TLS protocol version:

   ```
   web-server tls-min-ver [tlsv10 | tlsv11 | tlsv12]
   ```

4. Enable the Web server:

   ```
   web-server enable
   ```

5. Verify the protocol version:

   ```
   show web-server
   ```

Example

```
Switch> enable
Switch# configure terminal
Switch(config)# web-server tls-min-ver tlsv11
```

Verify the protocol version.

```
Switch> show web-server

Web Server Info :

        Status                    : on
        Secure-only               : disabled
        TLS-minimum-version       : tlsv11
        RWA Username              : admin
        RWA Password              : ********
        Def-display-rows          : 30
        Inactivity timeout        : 900 sec
        Html help tftp source-dir :
        HttpPort                  : 80
        HttpsPort                 : 443
        NumHits                   : 198
        NumAccessChecks           : 8
        NumAccessBlocks           : 0
        NumRxErrors               : 198
        NumTxErrors               : 0
```

```
        NumSetRequest              : 0
        Minimum password length    : 8
        Last Host Access Blocked   : 0.0.0.0
        In use certificate         : Self signed
```

Variable Definitions

Use the data in the following table to use the **web-server** command.

Variable	Value
def-display-rows <*10-100*>	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the Web interface. To disable the web server, use the no form of this command: `no web-server [enable]`
help-tftp <*WORD/0-256*>	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/help • 192.0.2.1:/
http-port <*80-49151*>	Configures the web server HTTP port. The default port is 80.
https-port <*443-49151*>	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout<*30–65535*>	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro | rwa} *WORD<1-20> WORD<1-32>*	Configures the logon and password for the web interface, where the first *WORD<1-20>* is the new logon and the second *WORD<1-32>* is the new password.
password min-passwd-len<*1–32*>	Configures the minimum password length. By default, the minimum password length is 8 characters.
read-only-user	Enables read-only user for the web server.
secure-only	Enables secure-only access for the web server.
tls-min-ver<*tlsv10|tlsv11|tlsv12*>	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2 The default is tlsv12.

Accessing the switch through the Web interface

Before you begin

You must enable the Web server using CLI.

About this task

Monitor the switch through a Web browser from anywhere on the network. The Web interface uses a 15-minute timeout period. If no activity occurs for 15 minutes, the system logs off the switch Web interface, and you must reenter the password information.

Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Note:

By default the Web server is configured with the secure-only option, which requires you to use HTTPS to access EDM. To access EDM using HTTP, you must disable the secure-only option. For more information about configuring the secure-only option, see Enabling the Web management interface on page 38.

Procedure

1. Start your Web browser.
2. Type the switch IP address as the URL in the Web address field.
3. In the **User Name** box type `admin` and **Password** box type `password`.
4. Click **Login**.

Configuring the minimum version of the TLS protocol

Use the following procedure to configure the minimum version of the TLS protocol.

Earlier releases used a self-signed certificate generated using the OpenSSL API, and this self-signed certificate was installed in `/inflash/.ssh`. The self-signed certificate is now generated with the Mocana API.

Disable the web server before changing the TLS version. By disabling the web server, other existing users with a connection to the web server are not affected by changing to a different version.

The switch by default supports version TLS 1.2 and above. You can explicitly configure TLS 1.0 and TLS 1.1 version support.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General** and select **Web** tab.

3. In the **TlsMinimumVersion** field, select the TLS version you want to configure as the minimum on the system.

Web field descriptions

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

Name	Description
WebRWAUserName	Specifies the RWA username from 1–20 characters. The default is admin.
WebRWAUserPassword	Specifies the password from 1–32 characters. The default is 12345678.
WebROEnable	Enables the web server read-only (RO) user, which is disabled by default after a software upgrade.
WebROUserName	Specifies the RO username from 1–20 characters. The default is user.
WebROUserPassword	Specifies the password from 1–32 characters. The default is password.
MinimumPasswordLength	Configures the minimum password length. By default, the minimum password length is 8 characters.
HttpPort	Specifies the HTTP port for web access. The default value is 80.
HttpsPort	Specifies the HTTPS port for web access. The default value is 443.
SecureOnly	Controls whether the secure-only option is enabled. The default is enabled.
InactivityTimeout	Specifies the idle time (in seconds) to wait before the EDM login session expires. The default value is 900 seconds (15 minutes).
TlsMinimumVersion	Configures the minimum version of the TLS protocol supported by the web-server. You can select from the following options: • tlsv10 – Configures the version to TLS 1.0. • tlsv11 – Configures the version to TLS 1.1. • tlsv12 – Configures the version to TLS 1.2 The default is tlsv12.
HelpTftp/Ftp_SourceDir	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/

Table continues…

Name	Description
	[<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 192.0.2.1:/Help • 192.0.2.1:/
DefaultDisplayRows	Configures the web server display row width between 10–100. The default is 30.
LastChange	Shows the last web-browser initiated configuration change.
NumHits	Shows the number of hits to the web server.
NumAccessChecks	Shows the number of access checks performed by the web server.
NumAccessBlocks	Shows the number of access attempts blocked by the web server.
LastHostAccessBlockedAddressType	Shows the address type, either IPv4 or IPv6, of the last host access blocked by the web server.
LastHostAccessBlockedAddress	Shows the IP address of the last host access blocked by the web server.
NumRxErrors	Shows the number of receive errors the web server encounters.
NumTxErrors	Shows the number of transmit errors the web server encounters.
NumSetRequest	Shows the number of set-requests sent to the web server.

Configuring a VLAN using CLI

Create a VLAN using CLI by port, protocol, or SPBM. Create a private VLAN by port. Optionally, you can choose to assign the VLAN a name and color.

Assign an IP address to the VLAN. You can also assign a MAC-offset value.

For more information on configuring a VLAN, see Configuring VLANs, Spanning Tree, and NLB for VOSS.

About this task

Create a VLAN and assign an IP address in CLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Create one of the following VLANs using CLI:
   - Create a port-based VLAN:

     ```
     vlan create <2-4059> [name WORD<0-64>] type port-mstprstp <0-63>
     [color <0-32>]
     ```

   - Create a VLAN using a user-defined protocol and specify the frame encapsulation header type:

     ```
     vlan create <2-4059> [name WORD<0-64>] type protocol-mstprstp <0-
     63> ipv6 [color <0-32>]
     ```

   - Create a spbm-bvlan VLAN:

     ```
     vlan create <2-4059>[name WORD<0-64>] type spbm-bvlan [color
     <0-32>]
     ```

   - Create a private-vlan VLAN:

     ```
     vlan create <2-4059> [name WORD<0-64>] type pvlan-mstprstp <0-63>
     secondary <2-4059>[color <0-32>]
     ```

3. Enter VLAN Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface vlan <1-4059>
   ```

4. Assign an IP address to a VLAN with or without specifying the MAC-offset. Do not assign an IP address to a spbm-bvlan or private-vlan type of VLAN.

   ```
   ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> [<0-511>]
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#vlan create 2 type port-mstprstp 6 color 4
Switch:1(config)#interface vlan 2
Switch:1(config-if)#ip address 192.0.2.40/24
```

Variable Definitions

Use the data in the following table to use the **`vlan create`** command.

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On

Table continues…

Variable	Value
	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.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional.
type port-mstprstp *<0-63> [color <0-32>]*	Creates a VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32. **Note:** MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.
type pvlan-mstprstp *<0-63> [color <0-32>]*	Creates a private VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp *<0–63>* ipv6	Creates a VLAN by protocol: • *<0–63>* is the STP instance ID. • color <0-32> is the color of the VLAN in the range of 0 to 32.
type spbm-bvlan	Creates a SPBM B-VLAN.

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

Variable	Value
<A.B.C.D/X>|<A.B.C.D> <A.B.C.D>	Specifies the IP address and subnet mask in the format A.B.C.D/X or A.B.C.D A.B.C.D.
<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 your switch, use the CLI command completion Help.

Use the data in the following table to use the **`vlan i-sid`** command.

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the

Table continues…

Variable	Value
	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.
<0-16777215>	Specifies the i-sid number. The value is in the range of <0-16777215>.

Configuring a VLAN using Enterprise Device Manager

Create a VLAN by port, protocol, or SPBM address using the Enterprise Device Manager (EDM). Additionally you can choose to assign the VLAN a name and a color.

Assign an IP address to the VLAN. You can also assign a MAC-offset value that ensures a given VLAN has the same MAC address across reboots.

Before you begin

Ensure you follow the VLAN configuration rules for the switch. For more information on the VLAN configuration rules and on configuring a VLAN, see Configuring VLANs, Spanning Tree, and NLB for VOSS.

About this task

Create a VLAN and assign an IP address to a VLAN to enable routing on the VLAN.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** box, type the VLAN name, or use the name provided.
6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.
7. In the **MstpInstance** box, click the down arrow and choose an msti instance from the list.
8. In the **Type** box, select the type of VLAN you want to create.
   - To create a VLAN by port, choose **byPort**.
   - To create a VLAN by protocol, choose **byProtocolId**. The supported protocol type is ipv6.
   - To create an SPBM B-VLAN, choose **spbm-bvlan**.
   - To create a private VLAN, choose **private**.

9. In the **PortMembers** box, click the **(...)** button.

   Note:

   This **PortMembers** box does not apply to all VLAN types.

10. Click on the ports to add as member ports.

    The ports that are selected are recessed, while the non-selected ports are not recessed. Port numbers that appear dimmed cannot be selected as VLAN port members.

11. Click **OK**.
12. Click **Insert**.
13. Close the **VLANs** tab.

    The VLAN is added to the **Basic** tab.

14. Assign an IP address to a VLAN to enable routing on the VLAN. In the Navigation tree, open the following folders: **Configuration** > **VLAN**.
15. Click **VLANs**.
16. In the **Basic** tab, select the VLAN for which you are configuring an IP address.
17. Click **IP**.

    The IP, Default tab appears.

18. Click **Insert**.
19. Configure the required parameters.
20. Click **Insert**.

Basic Field Descriptions

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

Name	Description
Id	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, 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.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color Identifier	Specifies a proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.

Table continues…

Name	Description
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
MstpInstance	Identifies the MSTP instance.
VrfId	Indicates the Virtual Router to which the VLAN belongs.
VrfName	Indicates the name of the Virtual Router to which the VLAN belongs.
PortMembers	Specifies the slot/port of each VLAN member. The sub-port only appears for channelized ports.
ActiveMembers	Specifies the slot/port of each VLAN member. The sub-port only appears for channelized ports.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN. The sub-port only appears for channelized ports.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN. The sub-port only appears for channelized ports.
ProtocolId	Specifies the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers of remote function call (RFC). If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.
AgingTime	Specifies the timeout period, in seconds, to age out dynamic members of this VLAN. This field only applies to policy-based VLANs. The default is 600.

Note:

If you or another user changes the name of an existing VLAN using the VLAN **Basic** tab (or using CLI), the new name does not initially appear in EDM. To display the updated name, perform one of the following actions:

- Refresh your browser to reload EDM.
- Log out of EDM and log in again to restart EDM.
- Click **Refresh** in the VLAN **Basic** tab toolbar. If the old VLAN name appears in other tabs, click **Refresh** on those tabs as well.

IP Address field descriptions

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

Name	Description
Interface	Shows the interface to which this entry applies.
Ip Address	Specifies the IP address to associate with the VLAN.
Net Mask	Specifies the subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits configured to 1 and all the hosts bits configured to 0.
BcastAddrFormat	Shows the IP broadcast address format on this interface.
ReasmMaxSize	Shows the size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	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	Indicates whether this entry corresponds to a brouter port, as oppose to a routable VLAN.
MacOffset	Specifies the MAC offset value. Routable VLANS are assigned MAC addresses arbitrarily or by offset. Their MAC addresses are: • 24 bits: Vendor ID • 12 bits: Chassis ID • 12 bits: 0xA00-0xFFF If you enter the MAC offset, the lowest 12 bits are 0xA00 plus the offset. If not, they are arbitrary.
VrfId	Associates the VLAN or brouter port with a VRF. VRF ID 0 is reserved for the administrative VRF.

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 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 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

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

Variable	Value
<a.b.c.d>	Specifies the IPv4 and IPv6 address of the TFTP server from which to copy the license file.
<file>	Specifies the name of the license file when copied to the flash. The destination file name must meet the following requirements: • Maximum of 63 alphanumeric characters • No spaces or special characters allowed • Underscore (_) is allowed • The file extension ".xml" is required
<srcfile>	Specifies the name of the license file on the TFTP server. For example, license.xml.

Use the data in the following table to help you install a license with 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

Saving the configuration

Save the configuration to a file to retain the configuration settings.

About this task

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

Note:

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

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

Example

```
Switch:1> enable
```

Save the file to the default location:

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

Backing up configuration files

Before and after you upgrade your switch software, make copies of the configuration files. If an error occurs, use backup configuration files to return the switch to a previous state.

Before you begin

- If you use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), ensure that you enable the FTP or TFTP server. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

About this task

Keep several copies of backup files.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Determine the configuration file names:

   ```
   show boot config choice
   ```

3. Save the configuration files. Assuming the files use the default file names, enter:

   ```
   save config
   ```

4. Copy the files to a safe place:

   ```
   copy /intflash/config.cfg /intflash/config_backup.cfg
   ```

```
copy /intflash/config.cfg a.b.c.d:/dir/config_backup.cfg
```

Example

Determine the configuration file names, save the configuration files, and copy the files to a safe place.

```
Switch:1>enable
Switch:1#show boot config choice
choice primary config-file "/intflash/config.cfg"
choice primary backup-config-file "/intflash/config.cfg"
Switch:1#save config
Switch:1#copy /intflash/config.cfg 00:11:f9:5b:10:42/dir/config_backup.cfg
Do you want to continue? (y/n)
y
```

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

Reset the switch:

```
Switch:1>enable
Switch:1#reset
Are you sure you want to reset the switch? (y/n)
y
```

Variable definitions

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

Table 13: Variable definitions

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

Installing a new software build

Use the following procedure to install a new software build for the switch.

For full upgrade instructions, see Administering VOSS.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

3. Install the image:

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

4. Restart the switch:

   ```
   reset
   ```

Example

Extract the release distribution files to the /intflash/release/ directory, extract the module files to the /intflash/release directory, and install the image.

```
Switch:1>enable
Switch:1#software add VSPX.X.X.X.X.tgz
Switch:1#software activate VSPX.X.X.X.X
Switch:1#reset
```

Removing a software build

Use the following procedure to remove a software build for the switch.

Important:

A maximum of 6 software distributions can be installed. Once the limit is reached, one or more distributions must be removed to accommodate new distributions.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Remove the software build:

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

Example

Remove the software build:

```
Switch:1>enable
Switch:1#software remove w.x.y.z
```

Chapter 5: Verification

This section contains information about how to verify that your provisioning procedures result in a functional switch.

Pinging an IP Device

About this task

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

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

A management instance ID can be specified to allow the OS 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>] [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 and mgmt interface only applies to hardware with a dedicated, physical management interface.

3. 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 | vlan]
   ```

Note:

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

Example

Ping an IP network connection through the management interface for IPv4, and for IPv6:

```
Switch:1>ping 192.0.2.2 vrf mgmtrouter
Switch:1>ping 2001:0db8:0000:0000:0000:0000:0000:0001 vrf mgmtrouter
```

Ping an IP device from a GRT VLAN IP interface:

```
Switch:1#ping 192.0.2.16
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

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

Variable	Value
count <1–9999>	Specifies the number of times to ping. The default is 1.
-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 | 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.
-I <1–60>	Specifies the interval between transmissions in seconds.

Table continues…

Variable	Value
	This parameter does not apply if you use the mgmt [clip | vlan] parameter.
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 • 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 | vlan] parameter.
mgmt [clip | vlan]	Specifies the Segmented Management Instance as the source for the outgoing ICMP ECHO packet. The packet goes out this specific interface only. 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.
-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 | 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 | vlan] parameter.
-t <1–120>	Specifies the no-answer timeout value in seconds. The default is 5.

Table continues…

Variable	Value
WORD<0–256>	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address.
vrf WORD<1–16>	Specifies the virtual router and forwarder (VRF) name. This parameter does not apply if you use the mgmt [clip | vlan] parameter.

Verifying boot configuration flags

Verify the boot configuration flags to verify boot configuration settings. Boot configuration settings only take effect after you reset the system. Verification of these parameters is essential to minimize system downtime and the resets to change them.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the flags:

   ```
   show boot config flags
   ```

Example

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 insight-port-connect-type vtd
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
```

Verifying the software release

About this task

Use CLI to verify your installed software. It is important to verify your software version before you place a device into a production environment.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the software release:

   ```
   show software detail
   ```

Example

The following is an example of the output of the `show software detail` command.

```
Switch:1#show software detail


================================================================================
                    software releases in /intflash/release/
================================================================================
VSPSwitch.X.X.X.X_GA
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int29
    ROOTFS                            2.6.32_int29
    APPFS                             VSPSwitch.X.X.X.X_GA
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VSPSwitch.X.X.X.X_GA  (Backup Release)
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int29
    ROOTFS                            2.6.32_int29
    APPFS                             VSPSwitch.X.X.X.X_GA
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VSPSwitch.X.X.X.X_GA  (Primary Release)
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int29
    ROOTFS                            2.6.32_int29
    APPFS                             VSPSwitch.X.X.X.X_GA
```

```
  AVAILABLE ENCRYPTION MODULES
    No Modules Added


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

Verifying the software version on the slots

Note:

This procedure only applies to VSP 8600 Series.

About this task

Use CLI to verify the software version running on each slot.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the software version running on each slot:

   ```
   show software slot
   ```

Example

The following is an example of the output of the **`show software slot`** command.

```
Switch:1#show software slot

================================================================================================
                          Software running on chassis

================================================================================================

Slot    Release

----    -------
1       VOSS8600.voss_4.5.0.0int011
2       VOSS8600.voss_4.5.0.0int011
4       VOSS8600.voss_4.5.0.0int011
SF 1    VOSS8600.voss_4.5.0.0int011
SF 2    VOSS8600.voss_4.5.0.0int011
```

Displaying local alarms

View local alarms to monitor alarm conditions.

Local alarms are raised and cleared by applications running on the switch. Local alarms are an automatic mechanism run by the system that do not require any additional user configuration. The

raising and clearing of local alarms also creates a log entry for each event. Check alarms occasionally to ensure no alarms require additional operator attention.

For more information, see Troubleshooting VOSS.

Procedure

Display local alarms:

```
show alarm database
```

Example

Display local alarms:

Note:

The switches that support SF cards display warning messages when SFIs are down.

```
Switch:1#show alarm database
      ALARM         EVENT          ALARM       ALARM                          CREATION  UPDATED         CLEARED
SLOT  ID            CODE           TYPE        STATUS       SEVERITY  FREQ    TIME      TIME            TIME        REASON
-------------------------------------------------------------------------------------------------------------------------------
CP1  00300001.238    0x0000c5e7    DYNAMIC       SET          INFO       1      [11/17/15 06:42:55.928]  [11/17/15 06:42:55.928]  [--/--/--
--:--:--.---]  Link Down(1/47)
CP1  00300001.239    0x0000c5e7    DYNAMIC       SET          INFO       1      [11/17/15 06:42:55.946]  [11/17/15 06:42:55.946]  [--/--/--
--:--:--.---]  Link Down(1/48)
CP1  00300001.241    0x0000c5e7    DYNAMIC       SET          INFO       1      [11/17/15 06:42:55.971]  [11/17/15 06:42:55.971]  [--/--/--
--:--:--.---]  Link Down(1/50)
CP1  00400005        0x000045e5    DYNAMIC       SET          INFO       1      [11/17/15 06:43:41.929]  [11/17/15 06:43:41.929]  [--/--/--
--:--:--.---]  Sending Cold-Start Trap
```

Displaying log files

Use this procedure to display log files.

Procedure

Display log files:

```
show logging file
```

Example

Display log files:

```
Switch:1>show logging file
CP1  [02/05/15 12:35:28.690:UTC] 0x00270428 00000000 GlobalRouter SW INFO Lifecy
cle: Start
CP1  [02/05/15 12:35:29.906:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s sockserv started, pid:4950
CP1  [02/05/15 12:35:29.907:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom95 started, pid:4951
CP1  [02/05/15 12:35:29.907:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom90 started, pid:4952
CP1  [02/05/15 12:35:29.908:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s imgsync.x started, pid:4953
CP1  [02/05/15 12:35:30.346:UTC] 0x0026452f 00000000 GlobalRouter SW INFO No pat
ch set.
CP1  [02/05/15 12:35:30.909:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s logServer started, pid:4996
CP1  [02/05/15 12:35:30.910:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s trcServer started, pid:4997
```

```
CP1  [02/05/15 12:35:30.910:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oobServer started, pid:4998
CP1  [02/05/15 12:35:30.911:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s cbcp-main.x started, pid:4999
CP1  [02/05/15 12:35:30.912:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s rssServer started, pid:5000
CP1  [02/05/15 12:35:30.912:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgServer started, pid:5001
CP1  [02/05/15 12:35:30.913:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgShell started, pid:5002
CP1  [02/05/15 12:35:30.914:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s coreManager.x started, pid:5003
CP1  [02/05/15 12:35:30.914:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s ssio started, pid:5004
CP1  [02/05/15 12:35:30.915:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s hckServer started, pid:5005
CP1  [02/05/15 12:35:30.916:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s remCmdAgent.x started, pid:5006
CP1  [02/05/15 12:35:32.910:UTC] 0x000006cc 00000000 GlobalRouter SW INFO rcStar
t:  FIPS Power Up Self Test SUCCESSFUL - 0
CP1  [02/05/15 12:35:32.911:UTC] 0x000006c2 00000000 GlobalRouter SW INFO rcStar
t:  Security Stack Init SUCCESSFUL - 0
CP1  [02/05/15 12:35:32.911:UTC] 0x000006c3 00000000 GlobalRouter SW INFO rcStar
t:  IPSEC Init SUCCESSFUL
CP1  [02/05/15 12:35:32.911:UTC] 0x000006bf 00000000 GlobalRouter SW INFO rcStar
t: Security Stack Log init SUCCESSFUL - 0
CP1  [02/05/15 12:35:34.330:UTC] 0x000005c0 00000000 GlobalRouter SW INFO Licens
eLoad = ZERO, loading premier license for developer debugging
IO1  [02/05/15 12:35:35.177:UTC] 0x0011054a 00000000 GlobalRouter COP-SW INFO De
tected Master CP in slot 1

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

Chapter 6: Next steps

For more information about documents on how to configure other switch features, see Documentation Reference for VOSS.

For more information on new features of the switch, and important information about the latest release, see Release Notes for VOSS.

For more information about how to configure security, see Configuring Security for VOSS.

For the current documentation, see the Extreme Networks documentation page: www.extremenetworks.com/documentation/.

Glossary

command line interface (CLI)	A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Data Terminating Equipment (DTE)	A computer or terminal on the network that is the source or destination of signals.
Enterprise Device Manager (EDM)	A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
File Transfer Protocol (FTP)	A protocol that governs transferring files between nodes, as documented in RFC 959. FTP is not secure and does not encrypt transferred data. Use FTP access only after you determine it is safe in your network.
Simple Network Management Protocol (SNMP)	SNMP administratively monitors network performance through agents and management stations.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.