Quick Start Configuration

Release 4.3
NN47500-501
Issue 01.01
March 2016

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: New in this document

Quick Start Configuration is a new document for Release 4.3 so all the features are new in this release. See *Release Notes* for a full list of features.

Chapter 2: Fundamentals

Provisioning follows hardware installation.

Quick Start Configuration includes the minimum, but essential, configuration steps to:

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

For more information about hardware specifications and installation procedures, see the hardware documentation for your platform.

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

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 **`spbm-config-mode`**.

- The **`spbm-config-mode`** boot 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 config and reboot with the saved config. When the flag is disabled, you can configure PIM and IGMP Snooping, but you cannot configure SPB or IS-IS.

Important:

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

For information about verifying boot flags, see Verifying boot configuration flags on page 47. For more information about this boot flag and Simplified vIST, see *Configuring IP Multicast Routing Protocols*.

System connection

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

The default communication protocol settings for the console port are

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

To use the console port, you need the following equipment:

- A terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.

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.

The administrator then configures default logins and passwords for the other users based on the role-based authentication levels of the user. For more information on system access fundamentals and configuration, see *Administering*.

Table 1: 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

Table continues…

Access level	Description	Default logon	Default password
Layer 3 read/write	View and change configuration and status information for Layer 2 and Layer 3 (routing) functions.	l3	l3
Read/write	View and change configuration and status information across the switch. 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 2: 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:** It is recommended that you 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 *Using CLI and EDM*.

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.

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

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.

If you experience any issues while connecting to the EDM, check the proxy settings. Proxy settings can 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.

Table 3: 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*.

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.

EDM window

The following figure shows 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.
- Menu bar—Located at the top of the window, the menu bar shows the most recently accessed primary tabs and their respective secondary tabs.
- Toolbar—Located just below the menu bar, the toolbar gives you quick access to the most common operational commands such as Apply, Refresh, and Help.
- Work area—Located on the right side of the window, the work area displays the dialog boxes where you can view or configure parameters on the switch.

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

Note:

The Device Physical View on your hardware type 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 Control Processor (CP) module. 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 24. 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 (RFC 1812). 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.

NLB unicast is not supported by all hardware platforms. For more information about feature support, see *Release Notes*.

Chapter 3: 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 "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
```

Connecting 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 RJ45 connector for the console port on the switch that is provided with 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.

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
   - 8 data bits
   - 1 stop bit
   - No parity
2. Connect the RJ45 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*.

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.

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

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

Variable	Value
access-level *WORD<2–8>*	Permits or blocks this access level. The available access level values are as follows: • 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.
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 4: 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

Table continues…

Variable	Value
	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.Companyname.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.

Table continues…

Variable	Value
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:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Save the changed configuration.

Example

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

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

Variable definitions

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

Table 5: Variable definitions

Variable	Value
WORD<1–10>	Specifies a directory name or a time zone name in /usr/share/zoneinfo, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter `clock time-zone` 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. Log on as rwa.
2. Enter Privileged EXEC mode:

   ```
   enable
   ```

3. Configure the date:

   ```
   clock set <MMddyyyyhhmmss>
   ```

4. 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 6: 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).

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

Before you begin

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

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface mgmtEthernet mgmt
   ```

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

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

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

   ```
   ipv6 interface address WORD<0-255>
   ```

4. Show the complete network management information:

```
show interface mgmtEthernet
```

5. Show the management interface packet/link errors:

   ```
   show interface mgmtEthernet error
   ```

6. Show the management interface statistics information:

   ```
   show interface mgmtEthernet statistics
   ```

Example

Configure the IP address for the management port:

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

Variable definitions

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

Variable	Value
{<*A.B.C.D/X*> | <*A.B.C.D*> <*A.B.C.D*>}	Specifies the IP address and 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 using CLI

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, see *Release Notes*.

Procedure

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

   ```
   enable
   ```

```
configure terminal
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 192.0.2.2 255.255.0.0 198.51.100.126 weight 20 preference 1
Switch:1(config)#ip route 192.0.2.2 255.255.0.0 198.51.100.126 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  255.255.255.0 198.51.100.126  GlobalRouter 20    1    TRUE    ACTIVE TRUE
```

Variable definitions

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

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.
enable	Adds a static route to the router or VRF.

Table continues…

Variable	Value
	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.

Variable	Value
<*A.B.C.D*>	Specifies the route by IP address.
-s { <*A.B.C.D*> <*A.B.C.D*> | default}	Specifies the route by IP address and subnet mask.
vrf *WORD*<*1-16*>	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.

For route scaling information, see *Release Notes*.

Procedure

1. In the navigation pane, 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. 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**.

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

Table continues…

Name	Description
	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.
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*.

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 7: 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.

Table continues…

Variable	Value
	The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.
sshd	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 46.140.54.40
Connecting to 46.140.54.40.....
Login: rwa
Password: rwa
```

Enabling 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<1-20>
   ```

   Important:

   The default passwords and community strings are documented and well known. Change the default passwords and community strings immediately after you first log on.

6. Save the configuration:

   ```
   save config
   ```

7. Display the web server status:

   ```
   show web-server
   ```

Example

Enable the secure-only web-server, and configure the access level to read-write-all, for a username of smith2 and the password to 90Go243.

```
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 password rwa smith2 90Go243
Switch:1(config)#show web-server

Web Server Info :

        Status                    : on
        Secure-only               : enabled
```

```
        RWA Username               : admin
        RWA Password               : ********
        Def-display-rows           : 30
        Inactivity timeout         : 900 sec
        Html help tftp source-dir :
        HttpPort                   : 80
        HttpsPort                  : 443
        NumHits                    : 22
        NumAccessChecks            : 3
        NumAccessBlocks            : 1
        NumRxErrors                : 20
        NumTxErrors                : 0
        NumSetRequest              : 0
        Last Host Access Blocked   : 0.0.0.0
```

Variable definitions

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

Variable	Value
def-display-rows *<10–100>*	Configures the web server display row width. The default is 30.
enable	Enables the web interface. The default is disabled. Use the no operator before this parameter, `no web-server enable`, to disable the web interface.
help-tftp *WORD<0–256>*	Configures the source location for Help files using the following format: a.b.c.d:/| intflash/ [<dir>]. The path can use 0–256 characters. The source directory can be TFTP or FTP server that is reachable from the switch, or a internal flash (/intflash). The string can use 0-256 characters. The following example paths illustrate the correct format: • 47.17.82.25:/Switch_help • /intflash/Switch_help
http-port *<80 | 1024-49151>*	Configures the web server HTTP port. The default port is 80.
https-port *<443 | 1024-49151>*	Configures the web server HTTPS port. The default port is 443.
inactivity-timeout*<30–65535>*	Configures the web-server login session inactivity timeout.
secure-only	Enables the secure-only option on the web-server. The default value for the secure-only option is enabled. Use the no operator before this parameter, `no web-server secure-only`, to disable the web-server.

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

Variable	Value
ro *WORD<1–20> WORD<1–20>*	The first instance of *WORD<1–20>* specifies the username, and second instance of *WORD<1–20>*,

Table continues…

Variable	Value
	specifies the password for the read-only access-level.
rw *WORD<1–20> WORD<1–20>*	The first instance of *WORD<1–20>* specifies the username, and second instance of *WORD<1–20>*, specifies the password for the read-write access-level.
rwa *WORD<1–20> WORD<1–20>*	The first instance of *WORD<1–20>* specifies the username, and second instance of *WORD<1–20>*, specifies the password for the read-write-all access-level.

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 31.

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 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*.

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>} [<0-127>]
   ```

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 46.140.54.40/24
```

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. The system reserves VLAN IDs 4060 to 4094 for internal use.
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.
[<0-511>]	Specifies the MAC-offset value. The value is in the range of 0–511.

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*.

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 pane, expand 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. The choice you make in this step determines the other fields that appear in this dialog box.
   - 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.
11. Click **OK**.
12. Click **Insert**.
13. Assign an IP address to a VLAN to enable routing on the VLAN. In the Navigation pane, expand the following folders: **Configuration** > **VLAN**.
14. Click **VLANs**.
15. In the **Basic** tab, select the VLAN for which you are configuring an IP address.
16. Click **IP**.
17. Click the **IP Address** tab.
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 for the VLAN.
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.
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.
ActiveMembers	Specifies the slot/port of each VLAN member.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
ProtocolId	Specifies the network protocol for protocol-based VLANs. • ip (IP version 6) If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.

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, do one of the following:

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

IP Address field descriptions

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

Name	Description
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.
Mac Offset	Specifies the MAC offset value. The range is 0–511.

Installing a license file

Before you begin

- You must enable the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server depending on which protocol you use to download the license file to the device.
- Ensure that you have the correct license file with the base MAC address of the switch on which you need to install the license. Otherwise, the system does not unblock the licensed features.

About this task

Install a license file on the switch to enable licensed features.

Note:

You can enable FTP or TFTP in the boot config flags and then initiate an FTP or a TFTP session from your workstation to put the file on the server running on the switch.

Procedure

1. From a remote station, or PC, use FTP or TFTP to download the license file to the device, and store the license file in the /intflash directory.
2. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

3. To load the license file, execute the following command:

   ```
   load-license
   ```

   Important:

   If the loading fails, or if the switch restarts and cannot locate a license file in the specified location, the switch cannot unlock the licensed features.

   Important:

   The license filename stored on a device must meet the following requirements:

   - Maximum of 63 alphanumeric characters
   - No spaces or special characters allowed
   - Underscore (_) is allowed
   - The file extension ".xml" is required

Example

Use FTP to transfer a license file from a PC to the internal flash on the device.

Note:

This example uses the Premier plus MACsec license. The MACsec feature is not supported by all hardware platforms. For information about feature support, see *Release Notes*.

```
C:\Users\jsmith>ftp 192.0.2.16
Connected to 192.0.2.16 (192.0.2.16).
220 FTP server ready
Name (192.0.2.16:(none)): rwa
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put premier_macsec.xml  /intflash/premier_macsec.xml
local: premier_macsec.xml remote: /intflash/premier_macsec.xml
227 Entering Passive Mode (192,0,2,16,4,2)
150 Opening BINARY mode data connection
226 Transfer complete
101 bytes sent in 2.7e-05 secs (3740.74 Kbytes/sec)
ftp>
```

Log in to the device and load the license. The following example shows a successful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1 [06/12/15 15:59:57.636:UTC] 0x000005bc 00000000 GlobalRouter SW INFO
License Successfully Loaded From </intflash/premier_macsec.xml> License Type -- PREMIER
+MACSEC
```

The following example shows an unsuccessful operation.

```
Switch:1(config)#load-license
Switch:1(config)#CP1  [06/12/15 15:58:48.376:UTC] 0x000006b9 00000000 GlobalRouter SW
INFO Invalid license file /intflash/license_Switch_example.xml  HostId is not Valid

CP1  [06/12/15 15:58:48.379:UTC] 0x000005c4 00000000 GlobalRouter SW INFO No Valid
License found.
```

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.

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 8: 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*.

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.

The image names in this example do not reflect a true release. For image names, see *Release Notes* for that release.

```
Switch:1>enable
Switch:1#software add VOSS-PL-AC-w.x.y.z.tgz
Switch:1#software activate w.x.y.z
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 4: 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, then 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, then the message indicates the address does not respond.

Procedure

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

   ```
   ping WORD<0-256> [-d] [-I <1-60>] [-s] [-t <1-120>] [count <1-9999>]
   [datasize {<28-9216> | <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 interface only applies to hardware with a dedicated, physical management interface.

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
```

Variable definitions

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

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

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. Specifies the address to ping.

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:

The advanced-feature-bandwidth-reservation and ipv6-mode flags do not apply to all hardware models.

```
Switch:1>enable
Switch:1#show boot config flags
flags advanced-feature-bandwidth-reservation disable
flags block-snmp false
flags debug-config false
flags enhancedsecure-mode false
flags debugmode false
flags factorydefaults false
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags reboot true
flags rlogind true
flags spanning-tree-mode mstp
flags spbm-config-mode
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags verify-config 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. Log on to the switch to enter User EXEC mode.
2. Verify the software release:

   ```
   show software detail
   ```

Example

The following is an example of the output of the **`show software detail`** command. This example does not use actual software image names so differs from what you see on a real switch.

```
Switch:1>show software detail


================================================================================
                    software releases in /intflash/release/
================================================================================
VOSS-PL-AC-w.x.y.z_GA
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int38
    ROOTFS                            2.6.32_int38
    APPFS                             VOSS-PL-AC-w.x.y.z_GA
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VOSS-PL-AC-a.b.c.d_GA  (Backup Release)
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int38
    ROOTFS                            2.6.32_int38
    APPFS                             VOSS-PL-AC-a.b.c.d_GA
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VOSS-PL-AC-e.f.g.h_GA  (Primary Release)
  MP
    UBOOT                             int009
    KERNEL                            2.6.32_int38
    ROOTFS                            2.6.32_int38
    APPFS                             VOSS-PL-AC-e.f.g.h_GA
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES


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

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*.

Procedure

Display local alarms:

```
show alarm database
```

Example

Display local alarms:

```
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 5: Next steps

For more information on switch features, and important information about the latest release, see *Release Notes*.

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

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.