AVAYA

Quick Start Configuration for Avaya Virtual Services Platform 8200

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://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

Comments? infodev@avaya.com

Chapter 1: Introduction

Purpose

The Quick Start Guide provides basic instructions to install the hardware and perform basic configuration of the Avaya Virtual Services Platform 8200 chassis and software.

Related resources

Documentation

See the *Documentation Reference for Avaya Virtual Services Platform 8200,* NN47227-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

- In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

• To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.

- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  ✳ **Note:**

  Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

Procedure

1. In an Internet browser, go to https://support.avaya.com.

2. Type your username and password, and then click **Login**.

3. Click **MY PROFILE**.

4. On the site toolbar, click your name, and then click **E Notifications**.
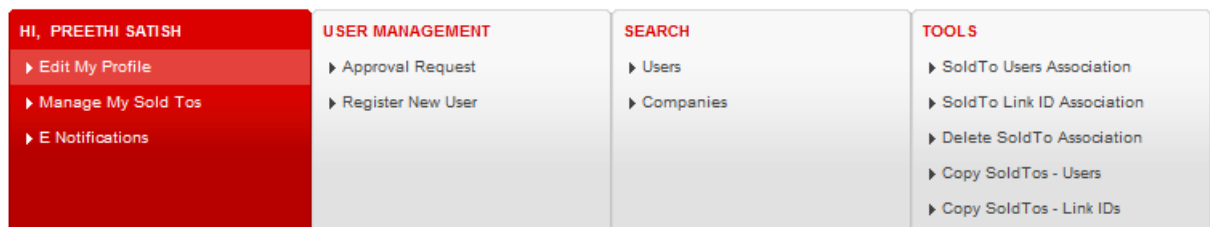
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.
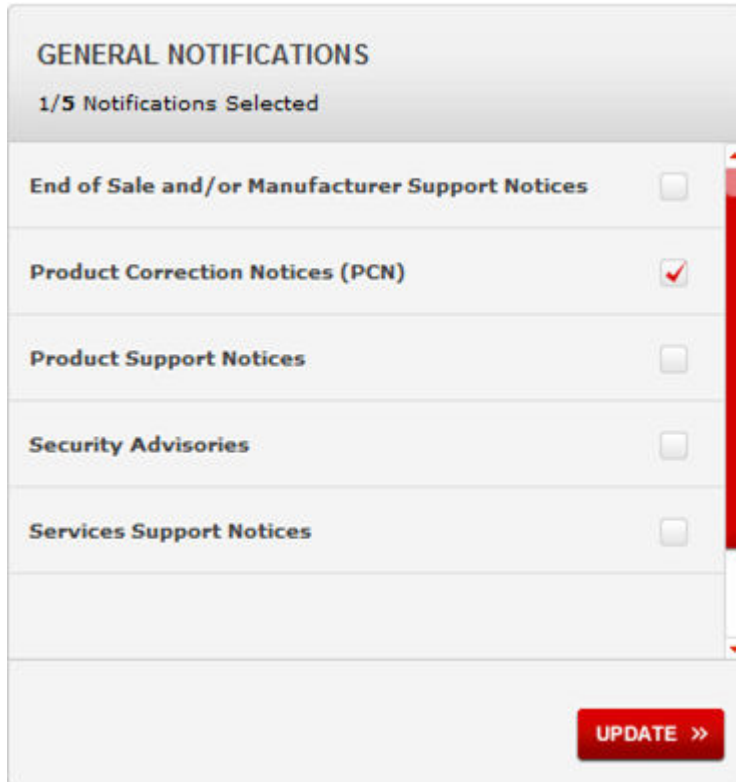
6. Click **OK**.

7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.
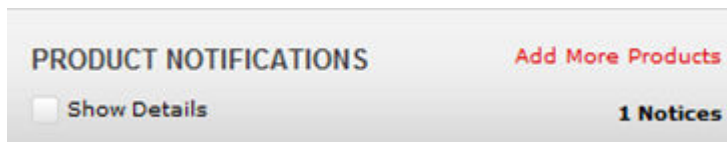
8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.

11. Click **Submit**.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>*.pdx.

3. In the Search dialog box, select the option **In the index named
   _<product_name_release>_.pdx**.

4. Enter a search word or phrase.

5. Select any of the following to narrow your search:

   • Whole Words Only

   • Case-Sensitive

   • Include Bookmarks

   • Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this release

The following sections detail what is new in *Quick Start Configuration for Avaya Virtual Services Platform 8200,* NN47227-102 for Release 4.1.

Features

See the following sections for information about feature changes.

Feature licenses

Release 4.1 adds feature license support. For information about how to install a license file, see Installing a license file on page 43.

IPv6 routing

Release 4.1 adds support for IPv6 routing. Existing information in this document is updated to include statements about IPv6 support for tools such as TFTP, FTP, HTTP, HTTPS, SSH, and ping.

Other changes

See the following sections for information about changes that are not feature-related.

Introduction chapter

The Introduction chapter has been updated to include information about subscribing to e-notifications and searching a documentation collection.

Chapter 3: Fundamentals

Provisioning follows hardware installation.

The *Quick Start Configuration for Avaya Virtual Services Platform 8200,* NN47227-102 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 *Installing the Avaya Virtual Services Platform 8200,* NN47227-300.

For more information about how to configure security, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

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, Avaya implemented a new 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 51. For more information about this boot flag and Simplified vIST, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.

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.

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
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

Table continues…

Access level	Description	Default logon	Default password
Read/write/all	Permits all the rights of read/write access and the ability to change security settings, including ACLI 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 Avaya Virtual Services Platform 8200 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	SCP	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	SSH v1, v2 Avaya recommends that you use SSHv2 instead of SSHv1.	Disabled
SNMPv1, SNMPv2	Enabled	SNMPv3 You must load the DES/AES image on the platform to use SNMPv3.For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.	Enabled
Rlogin	Disabled	Secure SHell (SSH) v1, v2	Disabled
HTTP	Disabled	HTTPS ❗ **Important:** Avaya recommends that you take the appropriate security precautions within the network if you use HTTP.	Enabled

Password encryption

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

> **Important:**
>
> For security reasons, Avaya recommends that you configure the passwords to values other than the factory defaults.

Enterprise Device Manager

Avaya Virtual Services Platform 8200 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 ACLI and EDM on Avaya Virtual Services Platform 8200,* NN47227-103.

Enterprise Device Manager access

To access EDM, open *http://<deviceip>/login.html* or *https://<deviceip>/login.html* from either Microsoft Internet Explorer 8.0, or Mozilla Firefox 7.x.

> **Important:**
>
> You must enable the Web server from ACLI 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. Avaya recommends that you 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 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 Avaya Virtual Services Platform 8200 using EDM. For more information about changing the Avaya Virtual Services Platform 8200 passwords, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

Table 3: EDM default username and password

Username	Password
admin	password

🛈 **Important:**

> The default passwords and community strings are documented and well known. Avaya strongly recommends that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

Device Physical View

After you access EDM, the first screen 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 port is up and running, red indicates the port is disabled, and amber indicates an enabled port that is not connected to anything. The chassis LEDs appear on the far right.

EDM window

The following figure shows the different sections of the EDM window:

- navigation tree—Located in the navigation pane on the left side of the window, the navigation tree displays all the available command tabs in a tree format. A row of buttons at the top of the navigation tree 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 Avaya Virtual Services Platform 8200.
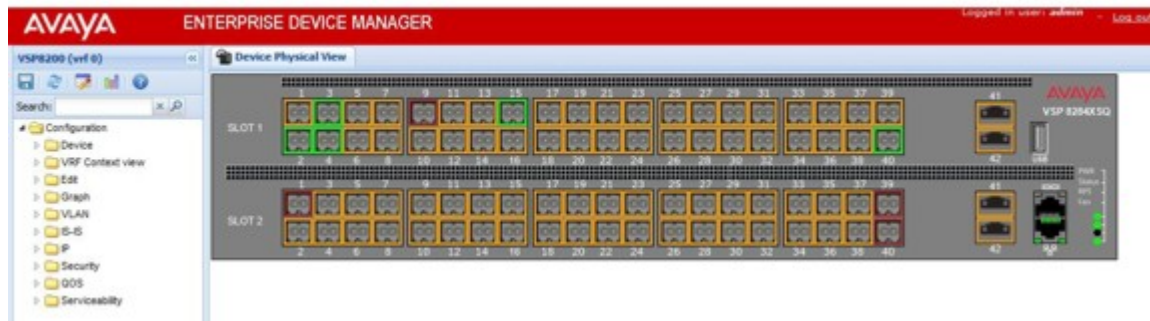
Figure 1: EDM window

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 28.

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 Avaya Virtual Services Platform 8200 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.

Chapter 4: Provisioning

This section contains procedures for the initial provisioning of Avaya Virtual Services Platform 8200. These procedures should always be performed when provisioning Avaya Virtual Services Platform 8200.

Configuring Avaya Virtual Services Platform 8200

You can use the information below to configure Avaya Virtual Services Platform 8200. The examples show you how to enable the access service, change the root level prompt, configure the ACLI logon banner, enable the web-server, and specify a gateway address route.

Before you begin

You must enable Global Configuration mode in ACLI.

About this task

Configure Avaya Virtual Services Platform 8200. 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 "VSP-CX"
banner custom
banner "Welcome to VSP 8200"
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
  - an cable with RJ45 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.

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 Avaya Virtual Services Platform 8200, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

If you enable the hsecure flag, after the aging time expires, the system prompts you to change your password. If you do not configure the aging time, the default is 90 days.

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 4: 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 5: 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.
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

`VSP-8284XSQ:1> enable`

`VSP-8284XSQ:1# configure terminal`

Change the system name:

`VSP-8284XSQ:1(config)# sys name Floor3Lab2`

Configure the system contact:

`Floor3Lab2:1(config)# snmp-server contact http://support.avaya.com/`

Configure the system location:

`Floor3Lab2:1(config)# snmp-server location "211 Mt. Airy Road, Basking Ridge, NJ 07920"`

Variable definitions

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

Table 6: 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. The default is support@avaya.com.
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,

Table continues…

Variable	Value
	use the default operator with the command. The default is an Avaya address.
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 ACLI 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 VSP 8200 default logon banner, 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 "Avaya, www.Avaya.com." and configure the message of the day to "Unauthorized access to this system is forbidden. Please logout now."

```
VSP-8284XSQ:1> enable
VSP-8284XSQ:1#configure terminal
VSP-8284XSQ:1(config)# banner custom
VSP-8284XSQ:1(config)# banner Avaya
VSP-8284XSQ:1(config)# banner www.Avaya.com
VSP-8284XSQ:1(config)# banner motd "Unauthorized access to this system is forbidden"
VSP-8284XSQ:1(config)# banner motd "Please logout now"
VSP-8284XSQ:1(config)#banner displaymotd
VSP-8284XSQ:1(config)#show banner
Avaya
www.avaya.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 ACLI 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

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data 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).

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

```
VSP-8284XSQ:1> enable
```

```
VSP-8284XSQ:1# configure terminal
```

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

```
VSP-8284XSQ: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 7: Variable definitions

Variable	Value
WORD<1–10>	Specifies a directory name or a time zone name. For example, Africa, Australia, Antarctica, or US. To see a list of options, enter

Table continues…

Variable	Value
	`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. For example, Shanghai in Asia. The second instance of *WORD<1–20>*is the subarea. 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 8: 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).

Before you begin

- Do not configure a default route in the Management VRF.
- If you want out-of-band management, Avaya recommends that you 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 VSP 8200 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.

⊛ **Note:**

For more information about the management port, see *Administering Avaya Virtual Services Platform 8200,*.

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

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

   ```
   ip address<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

```
VSP-8284XSQ:1> enable
```

```
VSP-8284XSQ:1# configure terminal
```

```
VSP-8284XSQ:1# interface mgmtethernet mgmt
```

Configure the IP address for the management port:

```
VSP-8284XSQ:1(config-if)# ip address 47.17.10.31 255.255.255.0
```

Variable definitions

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

Variable	Value
<A.B.C.D> <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 using ACLI

Before you begin

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

Procedure

1. Create an IP static route:

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

2. Enable an IP static route:

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

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

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

```
        show ip route static
```

5. Delete a static route:

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

The limit for a static route for VSP 8200 is 1000 per VRF and 5000 per system.

Example

```
VSP-8284XSQ:1> enable
```

Log on to Global Configuration mode:

```
VSP-8284XSQ:1# configure terminal
```

Log on to VRF Router Configuration mode:

```
VSP-8284XSQ:1# router vrf mgmtrouter
```

Create an IP static route:

```
VSP-8284XSQ:1(router-vrf)# ip route 42.17.0.0 255.255.0.0 42.17.156.126
weight 200
```

Enable a static route:

```
VSP-8284XSQ:1(router-vrf)# ip route 42.17.0.0 255.255.0.0 42.17.156.126
enable
```

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

```
VSP-8284XSQ:1(router-vrf)# show ip route static vrf mgmtrouter
```

Variable definitions

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

Table 9: 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

Table continues…

Variable	Value
	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 10: Variable definitions

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<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. The maximum number of static routes is 1000 per VRF and 5000 per system.

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.
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. In the **NextHopVrfId** field, select the appropriate value.
10. To enable the static route, select the **Enable** check box.
11. In the **Metric** field, type the metric.
12. In the **Preference** field, type the route preference.
13. 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.

Table continues…

Name	Description
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.
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 on Avaya Virtual Services Platform 8200,* NN47227-601.

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

`VSP-8284XSQ:1> enable`

`VSP-8284XSQ:1# configure terminal`

`VSP-8284XSQ:1(config)# boot config flags telnetd`

Variable definitions

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

Table 11: 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.

Table continues…

Variable	Value
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 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. 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. Avaya strongly recommends that you 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

```
VSP-8284XSQ:1> enable
```

```
VSP-8284XSQ:1# configure terminal
```

```
VSP-8284XSQ:1(config) web-server enable
```

```
VSP-8284XSQ:1(config) web-server secure-only
```

Configure the access level to read-write-all, for a username of smith2 and the password to 90Go243:

```
VSP-8284XSQ:1(config) web-server password rwa smith2 90Go243
```

Variable definitions

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

Table 12: Variable definitions

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 VSP 8200, or a internal flash (/ intflash). The string can use 0-256 characters. The following example paths illustrate the correct format: • 47.17.82.25:/VSP8200_help • /intflash/VSP8200_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.
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.

Table 13: Variable definitions

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>*, 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 ACLI.

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 36.

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 ACLI

Create a VLAN using ACLI 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 on Avaya Virtual Services Platform 8200,* NN47227-500.

About this task

Create a VLAN and assign an IP address in ACLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create one of the following VLANs using ACLI:

   - Create a port-based VLAN:

     ```
     vlan create <1-4059> [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 <1-4059> [name WORD<0-64>] type protocol-mstprstp <0-
     63> ipv6 [color <0-32>]
     ```

   - Create a spbm-bvlan VLAN:

     ```
     vlan create <1-4059> [name WORD<0-64>] type spbm-bvlan [color
     <0-32>]
     ```

   - Create a private-vlan VLAN:

     ```
     vlan create <1-4059> [name WORD<0-64>] type pvlan-mstprstp <0-63>
     secondary <1-4059>[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 2-4059. VLAN ID 1 is the default VLAN and cannot be created nor deleted. VLAN IDs 4060 to 4094 are reserved 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 Avaya Virtual Services Platform 8200. For more information on the VLAN configuration rules and on configuring a VLAN, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500.

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.

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

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 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 • bySpbm • byProtocolId
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.

Table continues…

Name	Description
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 ACLI), 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 Avaya Virtual Services Platform 8200 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 Avaya Virtual Services Platform 8200 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 VSP 8200.

Procedure

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

2. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   load-license
   ```

   ❗ **Important:**

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

   ❗ **Important:**

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

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

Example

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

```
C:\Users\jsmith>ftp 47.17.244.130
Connected to 47.17.244.130 (47.17.244.130).
220 FTP server ready
Name (47.17.244.130:(none)): rwa
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put licensefile.xml  /intflash/license.xml
local: licensefile.xml remote: /intflash/license.xml
227 Entering Passive Mode (47,17,244,130,4,2)
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:

```
VSP-8284XSQ:1(config)# load-license
```

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 VSP 8200 software, make copies of the configuration files. If an error occurs, use backup configuration files to return VSP 8200 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

Avaya recommends that you 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

```
VSP-8284XSQ> enable
```

Determine the configuration file names:

```
VSP-8284XSQ:1#show boot config choice
choice primary config-file "/intflash/config.cfg"
choice primary backup-config-file "/intflash/config.cfg"
```

Save the configuration files:

```
VSP-8284XSQ:1# save config
```

Copy the files to a safe place:

```
VSP-8284XSQ: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

```
VSP-8284XSQ:1> enable
```

Reset the switch:

```
VSP-8284XSQ: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 14: 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 Avaya Virtual Services Platform 8200.

Procedure

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

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

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

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

3. Install the image:

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

4. Restart the Avaya Virtual Services Platform 8200:

   ```
   reset
   ```

Removing a software build

Use the following procedure to remove a software build for Avaya Virtual Services Platform 8200.

🛈 **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>
```

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 Avaya Virtual Services Platform 8200 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 <28-51200>] [interface <gigabitEthernet|mgmtEthernet|
   tunnel|vlan] [scopeid <1-9999>] [Source WORD<1-256>][vrf WORD<0-16>]
   ```

Example

Ping an IP device through the management interface:

```
Switch:1> ping 47.17.41.20 vrf mgmtrouter
```

Ping an IPv6 device through the management interface:

```
Switch:1> ping 4717::7822:2 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|mgmtEthernet|tunnel|vlan	Specifies a specific outgoing interface to use by IP address. Additional ping interface filters: • gigabitEthernet: {slot/port} gigabit ethernet port • mgmtEthernet: mgmt • tunnel: tunnel ID as a value from 1 to 2000 • vlan: Specifies the VLAN ID in the range of 1-4059. VLAN IDs 1 to 4059 are configurable; VLAN IDs 4060 to 4094 are reserved for internal use. VLAN ID 1 is the default VLAN and cannot be created nor deleted.
-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<0–16>	Specifies the virtual router and forwarder (VRF) name from 1–16 characters.
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

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config 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 ACLI to verify your installed software. It is important to verify your software version before you place a device into a production environment.

Procedure

Verify the software release:

show software detail

Example

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

```
VSP-8k-R1-BEB-7:1(config)#show software detail
```

```
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP8K.4.1.0.0int031 (Backup Release)
    KERNEL                         2.6.32_int38
    ROOTFS                         2.6.32_int38
    APPFS                          VSP8K.4.1.0.0int031
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES


VSP8200.4.0.0.0.GA
    KERNEL                         2.6.32_int38
    ROOTFS                         2.6.32_int38
    APPFS                          VSP8200.4.0.0.0int056
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VSP8K.4.1.0.0int030
    KERNEL                         2.6.32_int38
    ROOTFS                         2.6.32_int38
    APPFS                          VSP8K.4.1.0.0int030
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES


VSP8200.4.1.0.0.GA (Primary Release)
    KERNEL                         2.6.32_int38
    ROOTFS                         2.6.32_int38
    APPFS                          VSP8K.4.1.0.0int031
  AVAILABLE ENCRYPTION MODULES
    No Modules Added



--------------------------------------------------------------------------------
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 Avaya Virtual Services Platform 8200,* NN47227-700.

Procedure

Display local alarms:

```
show alarm database
```

Example

```
VSP-8284XSQ:1#show alarm database
        ALARM               EVENT          ALARM        ALARM
CREATION
SLOT    ID                  CODE           TYPE         STATUS     SEVERITY
FREQ                  TIME                  N
--------------------------------------------------------------------------------
-------------------------
CP1  00400005          0x000045e5   DYNAMIC      SET          INFO        1      [01/05/70
23:10:09.171]  [01/05/70p
CP1  00000001          0x00000642   DYNAMIC      SET          INFO        1      [02/14/13
13:55:16.929]  [02/14/13.
```

Displaying log files

Use this procedure to display log files.

Procedure

Display log files:

```
show logging file
```

Example

```
VSP-8284XSQ:1>show logging file
CP1 [03/19/14 23:15:32.663] 0x0027042b 00000000 GlobalRouter SW INFO Process logger (for
process:lifecycle) started, pid:4769
CP1 [03/19/14 23:15:33.665] 0x00270428 00000000 GlobalRouter SW INFO Lifecycle: Start
CP1 [03/19/14 23:15:34.343] 0x0027042b 00000000 GlobalRouter SW INFO Process sockserv
started, pid:4778
CP1 [03/19/14 23:15:34.344] 0x0027042b 00000000 GlobalRouter SW INFO Process oom95
started, pid:4779
CP1 [03/19/14 23:15:34.345] 0x0027042b 00000000 GlobalRouter SW INFO Process oom90
started, pid:4780
CP1 [03/19/14 23:15:34.345] 0x0027042b 00000000 GlobalRouter SW INFO Process imgsync.x
started, pid:4781
CP1 [03/19/14 23:15:34.776] 0x0026452f 00000000 GlobalRouter SW INFO No patch set.
CP1 [03/19/14 23:15:35.346] 0x0027042b 00000000 GlobalRouter SW INFO Process logServer
started, pid:4829
CP1 [03/19/14 23:15:35.347] 0x0027042b 00000000 GlobalRouter SW INFO Process trcServer
started, pid:4830
CP1 [03/19/14 23:15:35.347] 0x0027042b 00000000 GlobalRouter SW INFO Process oobServer
started, pid:4831
CP1 [03/19/14 23:15:35.348] 0x0027042b 00000000 GlobalRouter SW INFO Process cbcp-main.x
started, pid:4832
CP1 [03/19/14 23:15:35.349] 0x0027042b 00000000 GlobalRouter SW INFO Process rssServer
started, pid:4833
CP1 [03/19/14 23:15:35.350] 0x0027042b 00000000 GlobalRouter SW INFO Process dbgServer
started, pid:4834
CP1 [03/19/14 23:15:35.350] 0x0027042b 00000000 GlobalRouter SW INFO Process dbgShell
started, pid:4835

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

Chapter 6: Next steps

For more information about documents on how to configure other Avaya Virtual Services Platform 8200 features, see *Documentation Reference for Avaya Virtual Services Platform 8200,* NN47227-100.

For more information on new features of the Avaya Virtual Services Platform 8200 and important information about the latest release, see *Release Notes for Avaya Virtual Services Platform 8284XSQ,* NN47227-401.

For more information about how to configure security, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

For the current documentation, see the Avaya Support Web site: www.avaya.com/support.

Comments? infodev@avaya.com

Glossary

Avaya command line interface (ACLI)
A textual user interface. When you use ACLI, 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.