Quick Start
Avaya Virtual Services Platform 9000

3.2
NN46250-102, 02.01
February 2012

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Purpose of this document

The Quick Start Guide provides basic instructions to install the hardware and perform basic configuration of the Virtual Services Platform 9000 chassis and software.

Chapter 2: New in this release

The following sections describe what is new in *Avaya Virtual Services Platform 9000 Quick Start*, NN46250–102.

Features

See the following section for information about feature changes.

IPv6 support

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

On IPv6 networks, VSP 9000 supports SSH server, remote login (rlogin) server and remote shell (rsh) server only. VSP 9000 does not support outbound SSH client over IPv6, remote login (rlogin) client over IPv6 or remote shell (rsh) client on IPv6. On IPv4 networks, VSP 9000 supports both the server and client for SSH, rlogin and rsh.

Other changes

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

Restructured document

The focus of *Avaya Virtual Services Program 9000 Quick Start*, NN46250–102, is changed from hardware installation to basic configuration. The *Avaya Virtual Services Program 9000 Quick Start*, NN46250–102, now explains how to connect Virtual Services Platform 9000 to the network and how to make VSP 9000 accessible remotely. Although commands are primarily on Avaya Command Line Interface (ACLI), there are some Enterprise Device Manager (EDM) procedures.

Retired document

The content in *Avaya Virtual Services Platform 9000 Quick Start*, NN46250–102, is moved from the *Avaya Virtual Services Platform 9000 Commissioning*, NN46250–300. The *Avaya Virtual Services Platform 9000 Commissioning*, NN46250–300, document is retired.

ACLI Commands

Examples for ACLI commands exist for most commands in the document.

Introduction chapter and navigation

Introduction chapters and navigation are removed .

Purpose of this document

To improve documentation usability, a brief description of the purpose of this document is now the first chapter.

Terminology

Terminology no longer exists in a separate document. Terminology is in a glossary at the end of this document.

Common procedures

Common procedures are incorporated into chapters throughout the document.

Chapter 3: Fundamentals

Provisioning follows hardware installation.

The *Avaya Virtual Services Platform 9000 Quick Start*, NN46250–102, includes the minimum, but essential, configuration steps to:

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

More information ships in the box with your new Virtual Services Platform 9000 chassis, including

- an installation kit
- a foldout poster, *Virtual Services Platform 9000 Chassis Installation*, 326110–A
- a poster for each interface module, *Virtual Services Platform 9000 Module Installation*, 325942–A.

For more information about hardware specifications and installation procedures, see *Avaya Virtual Services Platform 9000 Installation —Chassis*, NN46250–304.

For more information about how to configure security, see *Avaya Virtual Services Platform 9000 Security*, NN46250-601.

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

System connection

Connect the serial console interface (an RS-232 port) on the Control Processor (CP) module to a PC or terminal to monitor and configure the platform. The port uses a DB-9 connector. The following are the default communication protocol settings for the console port:

- 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.
- An Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 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.

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
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	rwa	rwa

Access level	Description	Default logon	Default password
	names and passwords and the SNMP community strings.		

Secure and nonsecure protocols

The following table describes the secure and nonsecure protocols that Virtual Services Platform 9000 supports.

Table 2: Secure and nonsecure protocols for IPv4 and IPv6

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
FTP and Trivial FTP **Note:** File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.	Disabled	SCP	Disabled
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 *Virtual Services Platform 9000 Series Security,* NN46250–601.	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.

Management port

You must assign an IP address to the management port before you can use it for out-of-band (OOB) management. In a platform with redundant CP modules, each management port uses a specific IP address. In addition, you can create a virtual management port with an IP address available to the master management module. The IP addresses assigned to the CP modules and the virtual management port must be in the same subnet.

The master management module replies to all management requests sent to the virtual IP address, and to requests sent to the management port IP address. If the master management module fails and the backup management module takes over, the virtual management port IP address continues to provide management access to the platform.

Enterprise Device Manager

Avaya Virtual Services Platform 9000 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 *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250-103.

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 Virtual Services Platform 9000 using EDM. For more information about changing the Virtual Services Platform 9000 passwords, see *Avaya Virtual Services Platform 9000 Security*, NN46250-601.

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 *Avaya Virtual Services Platform 9000 Security*, NN46250-601.

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, a module, 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 modules and 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 module, a port, a power supply, a fan module, 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 module 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, 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 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 Virtual Services Platform 9000.

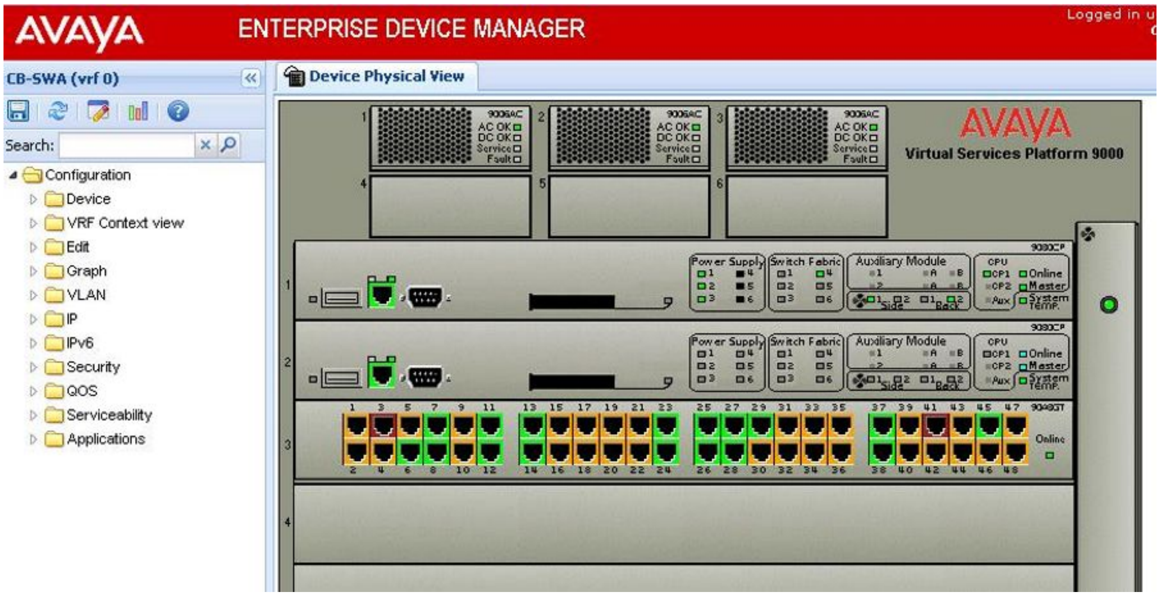

Figure 1: EDM window

Chapter 4: Provisioning

This section contains procedures for the initial provisioning of Virtual Services Platform 9000. These procedures should always be performed when provisioning Virtual Services Platform 9000.

Configuring Avaya Virtual Services Platform 9000

You can use the information below to configure Avaya Virtual Services Platform 9000. The examples show you how to enable the access service, change the root level prompt, configure the ACLI logon banner, enable the web-server, assign an IP address to the management port and specify a gateway address route.

For more information on where to find documents on how to configure other features on VSP 9000, see *Avaya Virtual Services Platform 9000 Documentation Roadmap*, NN46250–100.

Before you begin

You must enable Global Configuration mode in ACLI.

About this task

Configure Avaya Virtual Services Platform 9000. 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 9000"
banner displaymotd

web-server enable
no web-server secure-only
interface mgmtEthernet 1/1
ip address x.x.x.x 255.255.255.0
exit

interface mgmtEthernet 2/1
ip address x.x.x.x 255.255.255.0
exit

router vrf MgmtRouter
```

```
ip route 0.0.0.0 0.0.0.0 x.x.x.x  weight 1
exit
```

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 Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 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. Most computers or terminals use a male DB-25 connector.
- 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 RS-232 cable to the console port on the CP module.
3. Connect the other end of the RS-232 cable to the terminal or computer serial port.
4. Ensure that you shield the cable that connects to the console port to comply with emissions regulations and requirements.
5. Turn on the terminal.
6. Log on to the switch.

Specifying the primary CP

Before you begin

- You must enable at least Privileged EXEC mode in ACLI to use the show command in this procedure.
- You must enable the Global Configuration mode in ACLI to use the configuration command in this procedure.

About this task

Specify the primary CP to determine which CP you use as the master after the switch performs a full power cycle. After the CP becomes the primary, the master LED for the CP is on.

Procedure

1. View the current configuration for the primary CP:

   ```
   show boot config master
   ```

2. Specify the slot of the primary CP:

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

3. Save the configuration.
4. Restart the switch.

   ```
   reset [-y]
   ```

   Note:

   Using `-y` suppresses the confirmation message before the switch resets. If you omit this parameter, you must confirm the action before the switch resets.

Example

```
VSP-9012:1>enable

VSP-9012:1#boot config master 1

VSP-9012:1#save config file /mnt/intflash/ verbose

VSP-9012:1#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 `boot config master` command.

Table 4: Variable definitions

Variable	Value
1–2	Specifies the slot number for the primary CPU. This variable can be 1 or 2. The default primary is slot 1.

Changing passwords

Before you begin

- You must use an account with read-write-all privileges to change passwords. For security, the switch saves passwords to a hidden file.
- You must enable Global Configuration mode in ACLI.

About this task

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 9000, 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.

In hsecure mode, the master Control Processor (CP) module synchronizes the password aging time with the secondary CP module. After the password expires, you must change the password in the master CP module to log on to the secondary CP module.

Procedure

1. Change a password:

   ```
   cli password WORD<1–20> {layer1|layer2|layer3|read-only|
   read-write|read-write-all}
   ```

2. Enter the old password.
3. Enter the new password.
4. Enter the new password a second time.
5. 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

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Change a password:

```
VSP-9012:1(config)#cli password rwa read-write-all
```

Enter the old password:

```
VSP-9012:1(config)#rwa
```

Enter the new password:

```
VSP-9012:1(config)#summer
```

Enter the new password a second time:

```
VSP-9012:1(config)#summer
```

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

```
VSP-9012:1(config)#password access-level rwa aging-time 60
```

Variable definitions

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

Table 5: Variable definitions

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

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

Table 6: Variable definitions

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

Variable	Value
	• 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 IP address in the format a.b.c.d. • *<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

About this task

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

Procedure

1. Log on as rwa.
2. Enable Privileged EXEC mode in ACLI:
   `enable`
3. Enable Global Configuration mode in ACLI:
   `config {terminal|network}`
4. Change the system name:
   `sys name` *`WORD<0–255>`*
5. Configure the system contact:
   `snmp-server contact` *`WORD<0–255>`*
6. Configure the system location:
   `snmp-server location` *`WORD<0–255>`*

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Change the system name:

```
VSP-9012:1(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 7: 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

Variable	Value
	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, 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.

Before you begin

You must log on to the Global Configuration mode in ACLI.

About this task

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

Procedure

1. Configure the switch to use a custom banner or use the default banner:
   `banner <custom|static>`
2. Create a custom banner:
   `banner WORD<1-80>`

   Note:
   To provide a string with spaces, include the text in quotation marks.
3. Create the message-of-the-day:
   `banner motd WORD<1-1516>`
4. Enable the custom message-of-the-day:

```
banner displaymotd
```

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
VSP-9012:1#(config) banner custom
VSP-9012:1#(config) banner “Welcome to VSP 9000”
```

Variable definitions

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

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

Configuring the time zone

Before you begin

- You must enable the Global Configuration mode in ACLI.

About this task

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 from 1901 to 2038. You do not need to configure daylight savings.

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

Procedure

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

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

2. Save the changed configuration.

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

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

```
VSP-9012:1(config)# clock time-zone America Indiana Vevay
```

Variable definitions

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

Table 8: 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. Enable Privileged EXEC mode in ACLI:
   `enable`
3. Configure the date:
   `clock set <MMddyyyyhhmmss>`

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#clock set 11062011063030
```

Variable definitions

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

Table 9: Variable definitions

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

Assigning an IP address to the management port

Before you begin

- You must log on through the CP console, enter Global Configuration mode, and then navigate to `interface mgmtEthernet [1/1|2/1]` in ACLI.

About this task

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Procedure

1. Assign an IP address to the management port:
   `ip address {A.B.C.D} {A.B.C.D}`
2. Exit to Global Configuration mode.
3. Assign an IPv4 address to a virtual management port:
   `sys mgmt-virtual-ip {A.B.C.D/X}`
4. Assign an IPv6 address to a virtual management port:

```
ipv6 mgmt-virtual WORD<0-46>
```

5. Save the configuration.

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# interface mgmtEthernet 1/1

VSP-9012:1(config-if)# sys mgmt-virtual-ip
47.140.54.40/255.255.255.0

VSP-9012:1(config-if)# exit

VSP-9012:1(config)# sys mgmt-virtual-ip 47.140.54.60/255.255.255.0

VSP-9012:1(config)# save config

The physical and virtual IP must be in the same subnet.
```

Variable definitions

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

Table 10: Variable definitions

Variable	Value
{A.B.C.D} {A.B.C.D}	Specifies the IP address and subnet mask for the management port on the CP module. **Important:** You cannot assign an address of 0.0.0.0/0.

Use the data in the following table to use the `sys mgmt-virtual-ip` command.

Table 11: Variable definitions

Variable	Value
{A.B.C.D/X}	Specifies the IP address and subnet mask in the format A.B.C.D/x or A.B.C.D/x.x.x.x. (for example, 10.127.231.15/255.255.255.0). **Important:** You cannot assign an address of 0.0.0.0/0.

Use the data in the following table to use the `ipv6 mgmt-virtual` command.

Table 12: Variable definitions

Variable	Value
WORD<0–46>	Specifies the IPv6 address in hexadecimal format (string length 0–46) and the prefix-length.

Assigning static routes to the management interface

Before you begin

- You must log on through the CP console, enter Global Configuration mode, and then navigate to `router vrf mgmtRouter` in ACLI.

About this task

Assign a static route to specify a gateway address route for the management interface. You can specify up to four static routes for the management interface.

Procedure

1. Specify a gateway address route:

   ```
   ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1–65535>
   ```

2. Configure the preference for the route:

   ```
   ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1–255>
   ```

3. Enable the route with a local next hop:

   ```
   ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable
   ```

   If you configure this option, the static route becomes active only if the switch has a local route to the network.

4. Enable the route without a local next hop:

   ```
   ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable [next-hop-vrf
   WORD<0–16>]
   ```

5. Save the configuration.

Example

```
VSP-9012:> enable

VSP-9012:# configure terminal

VSP-9012:(config)# router vrf mgmtRouter 1/1
```

If you locate a management station on the network of 11.0.0.0/255.0.0.0, and the next hop to that network from the management interface is 10.127.231.1, enter the following command to specify a gateway management address route:

```
VSP-9012:1(router-vrf)# ip route 11.0.0.0 255.0.0.0 10.127.231.1
weight 1
```

The value 11.0.0.0 255.0.0.0 represents the target subnet; the value 10.127.231.1 represents the gateway used to point to the target subnet.

Variable definitions

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

Table 13: Variable definitions

Variable	Value
<1–65535>	Specifies the static route cost.
<1–255>	Indicates the route preference of this entry. If you can use more than one route to forward IP traffic, then the switch uses the route with the highest preference. The higher the number, the higher the preference.
{A.B.C.D} {A.B.C.D} {A.B.C.D}	Specifies the IP address, subnet mask, and next-hop address for the route. The first *{A.B.C.D}* configures the destination IP address of this route. An entry with a value of 0.0.0.0 is the default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries depends on the network management protocol table access mechanisms. The second *{A.B.C.D}* configures the route network mask with the destination address before the switch compares the mask to the destination value. The third *{A.B.C.D}* configures the IP address of the next hop of this route. In the case of a route bound to an interface realized through a broadcast media, the value of this box is the agent IP address on that interface.
WORD<0–16>	Specifies the VRF ID in inter-VRF static-route configuration.

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 *Avaya Virtual Services Platform 9000 Security*, NN46250-601.
- You must enable the Global Configuration mode in ACLI.

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, VSP 9000 supports SSH server and remote login (rlogin) server only. VSP 9000 does not support outbound SSH client over IPv6 or rlogin over IPv6. On IPv4 networks, VSP 9000 supports both server and client for SSH and rlogin.

Procedure

1. Enable the access service:
   ```
   boot config flags <ftpd|rlogind|sshd|telnetd|tftpd>
   ```
2. Repeat as necessary to activate the desired services.
3. Save the configuration.

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#boot config flags telnetd
```

Variable definitions

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

Table 14: 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

Variable	Value
	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.
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

Before you begin

- You must enable the Global Configuration mode in ACLI.

About this task

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

HTTP and HTTPS 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.

Procedure

1. Enable the Web server:

   ```
   web-server enable
   ```

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

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

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

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

4. 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.

5. Save the configuration:

   ```
   save config
   ```

6. Display the Web server status:

```
show web-server
```

Example

```
VSP-9012:1>enable
```

```
VSP-9012:#configure terminal
```

```
VSP-9012:1(config)web-server enable
```

```
VSP-9012:1(config)web-server secure-only
```

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

```
VSP-9012:1(config)web-server password rwa smith2 90Go243
```

Variable definitions

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

Table 15: 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 TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: • 47.17.82.25:/VSP9000_help • 47.17.82.25:/
http-port *<1–49151>*	Configures the Web server HTTP port. The default port is 80.
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 16: Variable definitions

Variable	Value
ro *WORD<1–20> WORD<1–20>*	Specifies first, the username, and second, the password for the read-only access-level.
rw *WORD<1–20> WORD<1–20>*	Specifies first, the username, and second, the password for the read-write access-level.
rwa *WORD<1–20> WORD<1–20>*	Specifies first, the username, and second, 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 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 ACLI

Create a VLAN using ACLI by IP subnet, port, protocol, or source MAC address. 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 that allows you to manually change the default MAC address.

For more information on configuring a VLAN, see *Avaya Virtual Services Platform 9000 Configuration — VLANs and Spanning Tree*, NN46250–500.

Before you begin

You must log on to Global Configuration mode in ACLI.

About this task

Create a VLAN and assign an IP address in ACLI.

Procedure

1. Create a VLAN using ACLI:
   ```
   vlan create <2–4084>
   ```
2. Specify a name for the VLAN:
   ```
   vlan create <2–4084> name WORD<0–64>
   ```
3. Create a VLAN by IP subnet:
   ```
   vlan create <2–4084> type ipsubnet-mstprstp <0–63> <A.B.C.D/
   X>
   ```
4. Create a VLAN by port:
   ```
   vlan create <2–4084> type port-mstprstp <0–63>
   ```
5. Create a VLAN by protocol:
   ```
   vlan create <2–4084> type protocol <0–63> {appleTalk|decLat|
   decOther|ip|netBios|PPPoE|rarp|sna802dot2|snaEthernet2|
   vines|xns}
   ```
6. Create a VLAN using a user-defined protocol and specify the frame encapsulation header type:
   ```
   vlan create <2–4084> type protocol-mstprstp <0–63>
   userDefined {0x000|<decimal value>} [encap{ethernet-ii|llc|
   snap}]
   ```
7. Create a VLAN by source MAC address:
   ```
   vlan create <2–4084> type srcmac-mstprstp <0–63>
   ```
8. Assign a color to the VLAN:
   ```
   vlan create <2–4084> type {ipsubnet-mstprstp <0–63> A.B.C.D/X
   [color <0–32>| port-mstprstp <0–63> [color <0–32>| protocol-
   ```

```
mstprstp <0–63>{appleTalk|decLat|decOther|ip|netBios|PPPoE|
rarp|sna802dot2|snaEthernet2|userDefined|vines|xns}[color
<0–32>]|srcmac-mstprstp <0–63> [color <0–32>]}
```

9. Log on to the VLAN Interface Configuration mode for the VLAN ID in ACLI:

   ```
   interface VLAN <2–4084>
   ```

10. Assign an IP address to a VLAN:

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

11. Specify the MAC-offset value:

    ```
    ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> [<0–1535>]
    ```

Example

```
VSP 9012:1> enable

VSP 9012:1# configure terminal

VSP 9012:1(config)# vlan create 2 type protocol 3 netBios color 4

VSP 9012:1(config)# interface vlan 2

VSP 9012:1(config-if)# ip address 46.140.54.40/24
```

Variable Definitions

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

Table 17: Variable definitions

Variable	Value
<2-4084>	Specifies the VLAN ID in the range of 2–4084.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional. **Note:** Do not use the name Mgmt when you specify a name for the VLAN that you create. VSP 9000 creates a management VLAN at boot up with the assigned name Mgmt. The show command does not show the management VLAN.

Variable	Value
type ipsubnet-mstprstp *<0-63> <A.B.C.D/X> [color <0-32]*	Creates a VLAN by IP subnet: • *<0-63>* is the STP instance ID in the range of 0–63. • *A.B.C.D/X* is the subnet address or mask {a.b.c.d/x | a.b.c.d/x.x.x.x}. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.
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.
type protocol-mstprstp *<0–63>* {appleTalk|decLat|decOther|ip|netBios|PPPoE|rarp|sna802dot2|snaEthernet2|vines|xns} *[color <0-32>]*	Creates a VLAN by protocol: • *<0–63>* is the STP instance ID. • appleTalk is the AppleTalk on Ethernet Type 2 and Ethernet SNAP frames Protocol. • decLat is the Digital Equipment Corporation Local Area Transport (DEC LAT) Protocol. • decOther is the DEC other Protocols. • ip is the Ip version 4 Protocol. • netbios is the NetBIOS Protocol. • PPPoE is the Point-to-Point Protocol Over Ethernet (PPPoE). • rarp is the Reverse Address Resolution Protocol (RARP). • sna802dot2 is the International Business Machines Systems Network Architecture (IBM SNA) on IEEE 802.2 frames. • snaethernet2 is the IBM SNA on Ethernet Type 2 frames. • vines is the Banyan VINES Protocol. • xns is the Xerox Network Systems Protocol. • color <0-32> is the color of the VLAN in the range of 0 to 32.

Variable	Value
type protocol-mstprstp *<0–63>* userDefined *{0x0000*|*<decimal value>}* [color] *<0-32>*] [encap {ethernet-ii|llc|snap}]	Creates a VLAN using a user defined protocol. • *<0-63>* is the STP instance ID in the range of 0–63. • *{0x0000*|*<decimal value>}* is the protocol ID in hexadecimal or decimal value. • color <0-32> is the color of the VLAN in the range of 0 to 32. • *encap* specifies the frame encapsulation header type.
type srcmac-mstprstp *<0-63>* [color *<0-32>*]	Creates a VLAN by source MAC address: • *<0-63>* is the STP instance ID in the range of 0–63. • color <0-32> is the color of the VLAN in the range of 0 to 32.

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

Table 18: Variable definitions

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.
[<0-1535>]	Specifies the MAC-offset value. The value is in the range of 0–1535.

Configuring a VLAN using Enterprise Device Manager

Create a VLAN by IP subnet, port, protocol, or source MAC address using Enterprise Device Manager (EDM). Optionally, 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 allows you to manually change the default MAC address.

Before you begin

Ensure you follow the VLAN configuration rules for Virtual Services Platform 9000. For more information on the VLAN configuration rules and on configuring a VLAN, see *Virtual Services Platform 9000 Configuration — VLANs and Spanning Tree*, NN46250–500.

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 IP Subnet, choose **byIPSubnet**. The fields needed to configure IP subnet-based VLANs are activated, including **SubnetAddr**, **SubnetMask**, and **AgingTime**.
    - To create a VLAN by protocol, choose **byProtocolId**. This activates additional fields to configure protocol-based VLANs, including a selection of various protocols.
    - To create a VLAN by source MAC, choose **bySrcMac**. The fields you require to configure the source MAC-based VLANs become active, including **AgingTime**.
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 • byIpSubnet • byProtocolId • bySrcMac
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.

Name	Description
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
OspfPassiveMembers	Specifies the slot/ports of each Open Shortest Path First (OSPF) passive member.
ProtocolId	Specifies the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers of remote function call (RFC). • ip (IP version 4) • ipx802dot3 (Novell Internetwork Packet Exchange (IPX) on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet Standard Network Access Protocol (SNAP) frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • appleTalk [AppleTalk on Ethernet Type 2 and Ethernet Symbolic Network Analysis Program (SNAP) frames] • decLat (Digital Equipment Corporation Local Area Transport (DEC LAT) protocol) • decOther (Other DEC protocols) • sna802dot2 (IBM SNA on IEEE 802.2 frames) • snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • rarp (Reverse Address Resolution Protocol) • PPPoE (Point-to-Point Protocol over Ethernet)

Name	Description
	If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.
SubnetAddr	Specifies the source IP subnet address (IP subnet-based VLANs only).
SubnetMask	Specifies the source IP subnet mask (IP subnet-based VLANs only).

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	Routable VLANS are assigned MAC addresses arbitrarily or by offset. Their MAC addresses are: • 24 bits: Avaya ID • 12 bits: Chassis ID • 12 bits: 0xA00-0xFFF If the MAC offset is entered, the lowest 12 bits will be 0xA00 plus the offset. If not, they will be arbitrary.

Installing a license file

Before you begin

- You must log on to Global Configuration mode in ACLI.
- File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
- Ensure that you have the correct license file with the base MAC address of the Virtual Services Platform 9000 on which you need to install the license. Otherwise, the system does not unblock the licensed features.
- If the chassis uses two CP modules, you do not need to install the license file on the secondary CP module. After you enable High Availability, the primary CP module copies the license vectors to the secondary CP module during table sync and the trial period countdown is stopped. This action ensures that the run time vectors of the primary and secondary CP module are the same. After you save the configuration on the primary CP module, the system copies the license file to the secondary CP module.

  In warm-standby mode, the system does not synchronize license vectors with the secondary CP module. However, the system copies the license file to the secondary CP module after you save the configuration with the save to standby flag configured as true.

About this task

Install a license file on Avaya Virtual Services Platform 9000 to enable licensed features.

Procedure

1. Install a license file:

   ```
   copy <a.b.c.d>:<srcfile> /intflash/<destfile>
   ```

   ```
   copy <x:x:x:x:x:x:x:x>:<srcfile> /intflash/<destfile>
   ```

2. Load the license file:

   ```
   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.

3. Save the configuration.

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Copy a license file from an IPv6 TFTP server to the flash on the CP module:

```
VSP-9012:1(config)# copy 4717:0:0:0:0:0:7834:3:license.lic /intflash/
license.dat
```

Load the license:

```
VSP-9012:1(config)# load-license
```

Variable definitions

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

Table 19: Variable definitions

Variable	Value
`<a.b.c.d>`	Specifies the IPv4 address of the TFTP server from which to copy the license file.
`<x:x:x:x:x:x:x:x:>`	Specifies the IPv6 address of the TFTP server from which to copy the license file. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
`<destfile>`	Specifies the name of the license file when copied to the flash. The destination file name must be lower case and have a file extension of .dat. For example, license.dat.
`<srcfile>`	Specifies the name of the license file on the TFTP server. For example, license.lic or license.dat. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Saving the configuration

After you change the configuration, you must save the changes to both the master and the standby CP modules. Save the configuration to a file to retain the configuration settings.

Before you begin

- You must log on to Privileged EXEC mode in ACLI.
- To save a file to the standby CP module, you must enable the Trivial File Transfer Protocol (TFTP) on the standby CP module.

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

Save the running configuration:

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

Example

```
VSP-9012:1>enable
```

Save the file to the default location:

```
VSP-9012:1#save config
```

Save the file as a backup file at a specified location:

```
VSP-9012:1#save config backup 4717:0:0:0:0:0:7933:6:/configs/
backup.cfg
```

Backing up configuration files

Before you begin

- If you use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), ensure that you enabled 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.
- You must log on to the Privileged EXEC mode in ACLI.

About this task

Before and after you upgrade your Avaya Virtual Services Platform 9000 software, make copies of the configuration files. If an error occurs, use backup configuration files to return Virtual Services Platform 9000 to a previous state.

Avaya recommends that you keep several copies of backup files.

Procedure

1. Determine the configuration file names:

   ```
   show boot config choice
   ```

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

```
save config
```

3. Save the configuration file to the secondary CP module if the SaveToStandby flag is false:

   ```
   save config standby config.cfg
   ```

4. Copy the files to a safe place:

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

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

Example

```
VSP-9012:1>enable
```

Determine the configuration file names:

```
VSP-9012:1#show boot config choice
choice primary config-file "/intflash/config.cfg"
choice primary backup-config-file "/intflash/config.cfg"
```

Save the configuration files:

```
VSP-9012:1#save config
```

Save the configuration file to the secondary CP module if the SaveToStandby flag is false:

```
VSP-9012:1#save config standby config.cfg
```

Copy the files to a safe place:

```
VSP-9012:1#copy /intflash/config.cfg fe81::222:5afe:fe68:c99d/dir/
config_backup.cfg
```

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

Resetting the platform

Before you begin

- You must log on to Privileged EXEC mode in ACLI.

About this task

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

Procedure

Reset the switch:

```
reset [-y]
```

Example

```
VSP-9012:1>enable
```

Reset the switch:

```
VSP-9012:1#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 20: 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.

Chapter 5: Verification

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

Pinging an IP device

Before you begin

- You must log on to User EXEC mode in ACLI.

About this task

Ping a device to test the connection between Avaya Virtual Services Platform 9000 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

Ping an IP network connection:

```
ping WORD<0–256> [-d] [-I <1–60>] [-s] [-t <1–120>] [count <1–
9999>] [datasize <16–65487>] [interface WORD <1–256>|
gigabitEthernet|mgmtEthernet|tunnel|vlan] [scopeid <1–9999>]
[scopeid <1–9999>] [vrf WORD<0–16>]
```

Example

Ping an IP device through the management interface:

```
VSP-9012:1>ping 4717::7822:2 vrf mgmtrouter
```

```
4717::7822:2 is alive
```

Variable definitions

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

Table 21: Variable definitions

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 *<16–65487>*	Specifies the size of ping data sent in bytes (16–65487). The default is 16.
interface *WORD <1–256>*|*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: {slot/port} management ethernet port • tunnel: tunnel ID as a value from 1 to 2147477248 • vlan: VLAN ID as a value from 1 to 4094
-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. Specify the MgmtRouter VRF if you need to run the ping operation through the management interface.
WORD *<0–256>*	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address (string length 0–256). Specifies the address to ping.

Verifying boot configuration flags

Before you begin

- You must be log on to Privileged EXEC mode.

About this task

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

Verify the flags:

```
show boot config flags
```

Example

```
VSP-9012:1>enable
VSP-9012:1#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags fabric-profile (1) Balanced
flags factorydefaults false
flags ftpd true
flags ha-cpu true
flags hsecure false
flags logging true
flags reboot true
flags rlogind true
flags spanning-tree-mode mstp
flags savetostandby true
flags sshd true
flags telnetd true
flags tftpd true
flags trace-logging false
flags verify-config false
flags wdt true
```

Verifying the software release

About this task

Use ACLI to verify your installed software after it has been upgraded. It is important to verify your software version before you place a device into a production environment.

For more information on upgrades and patches, see *Avaya Virtual Services Platform 9000 Upgrades and Patches*, NN46250–400. For the current documentation, see the Avaya Support Web site: www.avaya.com/support.

Procedure

Verify the software release:

`show software detail`

Example

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

```
VSP-9012:1#show software detail

===============================================================================
                    software releases in /intflash/release/
===============================================================================
asobalka-9772
  MP
    UBOOT                            int8
    KERNEL                           2.6.32_int13
    ROOTFS                           int330
    APPFS                            asobalka-9772
  IOP
    UBOOT                            int8
    KERNEL                           2.6.32_int13
    ROOTFS                           int330
    APPFS                            asobalka-9772
  IO_24PORT
    UBOOT                            int8
    KERNEL                           2.6.32_int13
    ROOTFS                           int330
    APPFS                            asobalka-9772
  IO_48PORT
    UBOOT                            int8
    KERNEL                           2.6.32_int13

    ROOTFS                           int330

    APPFS                            asobalka-9772

  SF

    UBOOT                            int26

    KERNEL                           2.6.32_int13

    ROOTFS                           int311

    APPFS                            asobalka-9772

  FPGA

    OXIDE                            10040918

    PHOSPHIDE                        10041310

    CATSKILL                         10052013

    ZAGROS                           11031817
    SULPHIDE                         10041310

    K2                               11072114

  AVAILABLE ENCRYPTION MODULES

No Modules Added
--More-- (q = quit)
```

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 *Avaya Virtual Services Platform 9000 Troubleshooting*, NN46250–700.

Procedure

Display local alarms:

```
show alarm database
```

Example

```
VSP-9012:1>show alarm database
  ALARM            EVENT         ALARM       ALARM
 CREATION             UPDATED             CLEARED
   ID              CODE          TYPE        STATUS     SEVERITY  FREQ
   TIME                TIME                 TIME                 REASON
--------------------------------------------------------------------------------
------------------------------------------------------------------------------
00000005.1      0x00000661    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:26]  [08/10/11 15:57:26]  [--/--/-- --:--:--]  Slot 1: Logging to int
ernal flash is not recommended - please insert external flash and ensure logging
 to external flash is con
00000003.1      0x0000065d    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:26]  [08/10/11 15:57:26]  [--/--/-- --:--:--]  Slot 1: Intflash disk
space utilization - above 75%, stop logging to file
00000006.1      0x000005a7    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:28]  [08/10/11 15:57:28]  [--/--/-- --:--:--]  No configured hosts ar
e reachable for log file transfer
0040000a.2      0x0001072b    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:33]  [08/10/11 15:57:33]  [--/--/-- --:--:--]  Unsupported Power Supp
ly Detected in slot PS 2.
0040000a.5      0x0001072b    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:33]  [08/10/11 15:57:33]  [--/--/-- --:--:--]  Unsupported Power Supp
ly Detected in slot PS 5.
00400006.3      0x000106cc    DYNAMIC       SET          WARNING    1      [08/1
0/11 15:57:33]  [08/10/11 15:57:33]  [--/--/-- --:--:--]  No fan module is prese
nt in slot SF-FAN 1
```

```
0040000b.9      0x00010755    DYNAMIC       SET          ERROR      3      [08/1
0/11 15:57:34]  [08/10/11 16:19:08]  [--/--/-- --:--:--]  Module 9024XL in slot
9 reached maximum failed reboots. Module has been powered down
00300001.258    0x0000c5e7    DYNAMIC       SET          INFO       1      [08/1
0/11 16:05:06]  [08/10/11 16:05:06]  [--/--/-- --:--:--]  Link Down(4/3)
00300001.260    0x0000c5e7    DYNAMIC       SET          INFO       1      [08/1
0/11 16:05:06]  [08/10/11 16:05:06]  [--/--/-- --:--:--]  Link Down(4/5)
09000005.1      0x002105a6    DYNAMIC       SET          WARNING    1      [08/1
0/11 16:05:06]  [08/10/11 16:05:06]  [--/--/-- --:--:--]  Slot 1, intflash disk
space used 1815240704 bytes, above 90% of total 2016641024 bytes
09200003.1      0x00248546    DYNAMIC       SET          WARNING    1      [08/1
0/11 16:05:06]  [08/10/11 16:05:06]  [--/--/-- --:--:--]  SYSTEM HAS 1 BME - No
Switch Fabric Redundancy Control !!!
00500001        0x000145e5    DYNAMIC       SET          INFO       5      [08/1
0/11 16:05:08]  [08/10/11 16:54:52]  [--/--/-- --:--:--]  New MSTP CIST Root 0x0
0247f9f6000 for instance 0
00400005        0x000045e5    DYNAMIC       SET          INFO       1      [08/1
0/11 16:05:52]  [08/10/11 16:05:52]  [--/--/-- --:--:--]  Sending Cold-Start Tra
p
```

Chapter 6: Next steps

For more information about documents on how to configure other Avaya Virtual Services Platform 9000 features, see *Avaya Virtual Services Platform 9000 Documentation Roadmap*, NN46250–100.

For more information on new features of the Virtual Services Platform 9000 and important information about the latest release, see *Avaya Virtual Services Platform 9000 Release Notes*, NN46250–401.

For more information on upgrades and patches, see *Avaya Virtual Services Platform 9000 Upgrades and Patches*, NN46250–400.

For more information about how to configure security, see *Avaya Virtual Services Platform 9000 Security*, NN46250-601.

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

Chapter 7: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

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

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

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.

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.