Quick Start- Avaya Virtual Services Platform 4000

Release 3.0.1.0
NN46251-102
Issue 02.01
July 2013

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

Warranty

Avaya provides a limited warranty on 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 website: 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, 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

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud

associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

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 website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

The Quick Start Guide provides basic instructions to install the hardware and perform basic configuration of the Virtual Services Platform 4000 chassis and software.

Related resources

Related topics:

Documentation on page 7
Training on page 7
Avaya Mentor videos on page 7

Documentation

See the *Avaya Virtual Services Platform 4000 Documentation Roadmap*, NN46251–100 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/.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://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 site.

Support

Visit 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.

Chapter 2: New in this release

The following sections detail what is new in *Avaya Virtual Services Platform 4000 Quick Start*, NN46251–500, for Release 3.0.1.0.

Features

See the following sections for information about feature-related changes.

Private VLAN

Release 3.0.1.0 introduces private VLANs. Private VLANs provide isolation between ports within a Layer 2 service.

For more information about private VLANs, see *Avaya Virtual Services Platform 4000 Configuration — VLANs and Spanning Tree*, NN46251-500.

Etree configuration

Release 3.0.1.0 introduces Etree configuration and private VLANs. Private VLANs consist of a primary and secondary VLAN. Etree allows the private VLANs to traverse a SPBM network by associating a private VLAN with an I-SID.

For more information about Etree configuration, see *Avaya Virtual Services Platform 4000 Configuration - Shortest Path Bridging MAC (SPBM)*, NN46251-510.

Chapter 3: Fundamentals

Provisioning follows hardware installation.

The *Avaya Virtual Services Platform 4000 Quick Start*, NN46251–102, 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 *Avaya Virtual Services Platform 4000 Installation*, NN46251–300.

For more information about how to configure security, see *Avaya Virtual Services Platform 4000 Security*, NN46251-601.

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 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
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 Virtual Services Platform 4000 supports.

Table 2: Secure and nonsecure protocols for IPv4

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
FTP and Trivial FTP	Disabled	SCP	Disabled

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
Note: File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support IPv4			
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 4000 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.

Enterprise Device Manager

Avaya Virtual Services Platform 4000 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 4000 User Interface Fundamentals*, NN46251-103.

Related topics:

Enterprise Device Manager access on page 14
Default user name and password on page 14
Device Physical View on page 15
EDM window on page 15

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 4000 using EDM. For more information about changing the Virtual Services Platform 4000 passwords, see *Avaya Virtual Services Platform 4000 Security*, NN46251-601.

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 4000 Security*, NN46251-601.

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 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 port or the entire chassis. To select an object, click the object. EDM outlines the selected object in yellow, indicating your selection.

The conventions on the device view are similar to the actual device appearance. The port LEDs and the ports are color-coded to provide status. Green indicates the module or port is up and running, red indicates the module or port is disabled, and amber indicates an enabled port that is not connected to anything. The chassis LEDs appear on the far left.

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 4000.

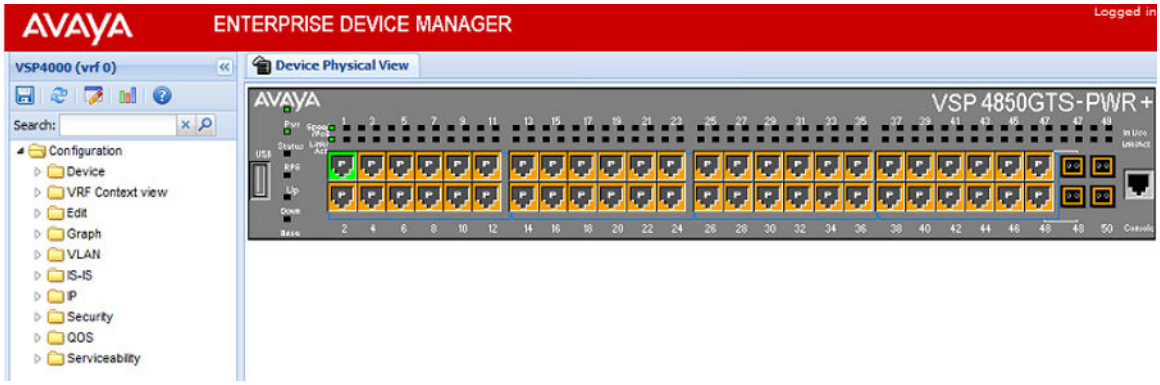

Figure 1: EDM window

Chapter 4: Provisioning

This section contains procedures for the initial provisioning of Virtual Services Platform 4000. These procedures should always be performed when provisioning Virtual Services Platform 4000.

Configuring Avaya Virtual Services Platform 4000

You can use the information below to configure Avaya Virtual Services Platform 4000. 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 4000. You can copy and paste the configuration in the example or modify it as desired.

Example

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

```
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 4000"
banner displaymotd

web-server enable
no web-server secure-only

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.

```
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 4000"
banner displaymotd

web-server enable
no web-server secure-only

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

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 4000, 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.

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. Re-enter the new password.
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-4850GTS>enable

VSP-4850GTS#configure terminal
```

Change a password:

```
VSP-4850GTS(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:

```
VSP-4850GTS(config)#password access-level rwa aging-time 60
```

Related topics:

Variable definitions on page 20

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.
password *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.

Variable	Value
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-4850GTS>enable

VSP-4850GTS#configure terminal
```

Change the system name:

```
VSP-4850GTS(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"
```

Related topics:

Variable definitions on page 22

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, 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 4000 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-4850GTS> enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)# banner custom
VSP-4850GTS(config)# banner Avaya
VSP-4850GTS(config)# banner www.Avaya.com
VSP-4850GTS(config)# banner motd "Unauthorized access to this system is forbidden"
VSP-4850GTS(config)# banner motd "Please logout now"
VSP-4850GTS(config)#banner displaymotd
VSP-4850GTS(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
```

Related topics:

Variable definitions on page 24

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 up to the year 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-4850GTS> enable

VSP-4850GTS# configure terminal
```

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

```
VSP-4850GTS(config)# clock time-zone America Indiana Vevay
```

Related topics:

Variable definitions on page 25

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 in `/usr/share/zoneinfo`, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter `clock time-zone`

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

Configuring the date

About this task

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

Procedure

1. Log on as rwa.
2. Enter Privileged EXEC mode:
   `enable`
3. Configure the date:
   `clock set <MMddyyyyhhmmss>`
4. Verify the configuration:
   `show clock`

Example

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

```
VSP-4850GTS>enable
VSP-4850GTS#clock set 02282013193030
Clock time has been set succesfully
VSP-4850GTS#show clock
Wed Feb 27 19:30:32 2013 EDT
```

Related topics:

Variable definitions on page 27

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.

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 4000 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 IPv4.

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-4850GTS>enable

VSP-4850GTS#configure terminal

VSP-4850GTS(config)#boot config flags telnetd
```

Related topics:

Variable definitions on page 28

Variable definitions

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

Table 9: Variable definitions

Variable	Value
ftpd	Enables the File Transfer Protocol remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
rlogind	Enables the rlogin remote-access service type. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
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 IPv4 addresses.

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-4850GTS>enable

VSP-4850GTS#configure terminal

VSP-4850GTS(config)web-server enable

VSP-4850GTS(config)web-server secure-only
```

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

```
VSP-4850GTS(config)web-server password rwa smith2 90Go243
```

Related topics:

Variable definitions on page 30

Variable definitions

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

Table 10: 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

Variable	Value
	VSP 4000, or a internal flash (/intflash). The string can use 0-256 characters. The following example paths illustrate the correct format: • 47.17.82.25:/VSP4000_help • /intflash/VSP4000_help
http-port *<80–1024-49151>*	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 11: 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 IPv4 addresses.

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 29.

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 *Avaya Virtual Services Platform 4000 Configuration — VLANs and Spanning Tree*, NN46251–500.

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 one of the following VLANs using ACLI:
   - Create a port-based VLAN:

     ```
     vlan create <2-4084> [name WORD<0-64> type port-mstprstp
     <0-63> [color <0-32>]
     ```

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

```
vlan create <2-4084> [name WORD<0-64>] type protocol-
mstprstp <0-63> ipv6 [color <0-32>]
```

- Create a spbm-bvlan VLAN:

```
vlan create <2-4084> [name WORD<0-64>] type spbm-bvlan
<0-63> [color <0-32>]
```

- Create a private-vlan VLAN:

```
vlan create <2-4084> [name WORD<0-64>] type pvlan-
mstprstp <0-63> secondary <2-2084> [color <0-32>]
```

2. Log on to the VLAN Interface Configuration mode for the VLAN ID in ACLI:
   `interface VLAN <2-4084>`
3. 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

```
VSP-4850GTS> enable

VSP-4850GTS# configure terminal

VSP-4850GTS(config)# vlan create 2 type port-mstprstp 6 color 4

VSP-4850GTS(config)# interface vlan 2

VSP-4850GTS (config-if)# ip address 46.140.54.40/24
```

Related topics:

Variable Definitions on page 33

Variable Definitions

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

Table 12: Variable definitions

Variable	Value
<2-4084>	Specifies the VLAN ID in the range of 2–4084. **Note:** VLANs 4061-4084 are reserved for internal use in Release 3.0.1.0. If you

Variable	Value
	attempt to configure a VLAN in this range, the following message appears: `Error: Invalid Vlan Id. Vlan 4061 to 4084 is being used internally.`
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.

Table 13: 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.
[<0-127>]	Specifies the MAC-offset value. The value is in the range of 0–127.

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 allows you to manually change the default MAC address.

Before you begin

Ensure you follow the VLAN configuration rules for Virtual Services Platform 4000. For more information on the VLAN configuration rules and on configuring a VLAN, see *Virtual Services Platform 4000 Configuration — VLANs and Spanning Tree*, NN46251–500.

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**.

Related topics:

Basic field descriptions on page 36

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.

Name	Description
VrfName	Indicates the name of the Virtual Router to which the VLAN belongs.
PortMembers	Specifies the slot/port of each VLAN member.
ActiveMembers	Specifies the slot/port of each VLAN member.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
ProtocolId	Specifies the network protocol for protocol-based VLANs. • ip (IP version 6) If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.

Note:

If you or another user changes the name of an existing VLAN using the VLAN **Basic** tab (or using 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 0–127.

Installing a license file

Before you begin

- You must log on to the Global Configuration mode in ACLI.
- 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 Virtual Services Platform 4000 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 4000 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 4000.

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. Log in to the device and enter the global configuration mode:

   ```
   VSP-4850GTS:> enable
   VSP-4850GTS:# configure terminal
   ```

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

   ```
   VSP-4850GTS:(confi)# 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
   - Lowercase only
   - No spaces or special characters allowed
   - Underscore (_) is allowed

- The file extension ".dat" is required

Example

Ftp 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.dat  /intflash/license.dat
local: licensefile.dat remote: /intflash/license.dat
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-4850GTS-PWR+:(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 IPv4 addresses.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. Save the running configuration:
   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

Save the file to the default location:

```
VSP-4850GTS>enable
VSP-4850GTS#save config
```

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 IPv4 addresses.
- You must log on to the Privileged EXEC mode in ACLI.

About this task

Before and after you upgrade your Avaya Virtual Services Platform 4000 software, make copies of the configuration files. If an error occurs, use backup configuration files to return Virtual Services Platform 4000 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. 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-4850GTS>enable
```

Determine the configuration file names:

```
VSP-4850GTS#show boot config choice
choice primary config-file "/intflash/config.cfg"
choice primary backup-config-file "/intflash/config.cfg"
```

Save the configuration files:

```
VSP-4850GTS#save config
```

Copy the files to a safe place:

```
VSP-4850GTS#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

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-4850GTS>enable
```

Reset the switch:

```
VSP-4850GTS#reset
Are you sure you want to reset the switch? (y/n)y
```

Related topics:

Variable definitions on page 41

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 Virtual Services Platform 4000.

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 Virtual Services Platform 4000:
   `reset`

Installing a module to a release

Use the following procedure to add a module to a release for Virtual Services Platform 4000.

Procedure

1. Download the module file to the device.
2. Extract/add the module files to the /intflash/release directory:
   `Software add-module [software version] [modules file name]`

Example

Ftp a module file from a remote station (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 VSP4K.3.0.1.0_modules.tgz
```

```
local: VSP4K.3.0.1.0_modules.tgz remote: VSP4K.3.0.1.0_modules.tgz
227 Entering Passive Mode (47,17,244,130,4,3)
150 Opening BINARY mode data connection
226 Transfer complete
37795 bytes sent in 0.237 secs (159.78 Kbytes/sec)
ftp>
```

Extract and add the module file to the release directory:

```
VSP-4850GTS:1#software add-modules 3.0.1.0.GA VSP4K.3.0.1.0_modules.tgz
Extracting module information from /media/sda3/intflash/VSP4K.3.0.1.0_modules.tgz
Unpacking /media/sda3/intflash/VSP4K.3.0.1.0_modules.tgz to /intflash/release/
3.0.1.0.GA/modules/.
Successfully unpacked /media/sda3/intflash/VSP4K.3.0.1.0_modules.tgz to /intflash/
release/3.0.1.0.GA/modules/.
VSP-4850GTS:1#
```

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 4000 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 <28-51200>] [interface WORD <1-256>| gigabitEthernet|tunnel|vlan] [vrf WORD<0-16>]
```

Example

Ping an IP device through the management interface:

```
VSP-4850GTS>ping 47.17.41.20 vrf vrf1
```

Related topics:

Variable definitions on page 45

Variable definitions

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

Table 15: 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 *<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 *WORD <1–256>*|*gigabitEthernet*|*tunnel*|*vlan*	Specifies a specific outgoing interface to use by IP address. Additional ping interface filters: • gigabitEthernet: {slot/port} gigabit 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.
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). 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-4850GTS>enable
VSP-4850GTS#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 logging true
flags reboot true
flags rlogind true
flags spanning-tree-mode mstp
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. 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.

```
VVSP-4850GTS-PWR+:1#show software
detail

================================================================================
                    software releases in /intflash/release/
================================================================================
VSP4K.3.0.1.0int017
  MP
    UBOOT                           int009
    KERNEL                          2.6.32_int29
    ROOTFS                          2.6.32_int29
    APPFS                           VSP4K.3.0.1.0int017
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VSP4K.3.0.1.0int024 (Backup Release)
  MP
    UBOOT                           int009
    KERNEL                          2.6.32_int29
    ROOTFS                          2.6.32_int29
    APPFS                           VSP4K.3.0.1.0int024
  AVAILABLE ENCRYPTION MODULES
    No Modules Added

VSP4K.3.0.1.0int038 (Primary Release)
  MP
    UBOOT                           int009
    KERNEL                          2.6.32_int29
    ROOTFS                          2.6.32_int29
    APPFS                           VSP4K.3.0.1.0int038
  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 *Avaya Virtual Services Platform 4000 Troubleshooting*, NN46251–700.

Procedure

Display local alarms:

```
show alarm database
```

Example

```
VSP-4850GTS-PWR+: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.
```

Chapter 6: Next steps

For more information about documents on how to configure other Avaya Virtual Services Platform 4000 features, see *Avaya Virtual Services Platform 4000 Documentation Roadmap*, NN46251–100.

For more information on new features of the Virtual Services Platform 4000 and important information about the latest release, see *Avaya Virtual Services Platform 4000 Release Notes*, NN46251–401.

For more information about how to configure security, see *Avaya Virtual Services Platform 4000 Security*, NN46251–601.

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