



Quick Start Configuration for Avaya Ethernet Routing Switch 4800 Series

Release 5.9
NN47205-104
Issue 03.02
August 2016

Notice

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

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR

IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment.

Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel,

or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction	7
Purpose.....	7
Chapter 2: New in this release	8
Features.....	8
Other changes.....	8
Chapter 3: Fundamentals	9
System connection.....	9
System Logon.....	10
Secure and nonsecure protocols.....	10
Management port.....	11
Password encryption.....	12
Enterprise Device Manager.....	12
Chapter 4: Connecting to the switch	16
Connecting a terminal to the switch.....	16
Configuring the terminal.....	18
Chapter 5: Configuring the switch using ACLI	19
Configuring the management IP address.....	19
Configuring BootP on the current instance of the switch or server.....	20
Setting user access limitations.....	21
Setting the read-only and read/write passwords.....	21
Enabling and disabling passwords.....	22
Setting user access limitations using Enterprise Device Manager.....	23
Configuring the console password using EDM.....	23
Configuring the web and telnet password using EDM.....	24
Configuring the ACLI banner.....	25
Configuring system identification.....	27
Enabling logging.....	29
Configuring Simple Network Time Protocol.....	29
Configuring local time zone.....	30
Configuring the clock.....	32
Configuring a static route.....	33
Enabling remote access.....	34
Using telnet to log on to the device.....	35
Enabling the web server management interface.....	35
Accessing the switch through the web interface.....	36
Configuring a VLAN.....	37
Configuring VLAN using EDM.....	40
Installing a license file.....	42
Saving the configuration.....	43

Storing the configuration files.....	43
Chapter 6: Verification	47
Pinging an IP device.....	47
Verifying the software release.....	47
Displaying local alarms.....	48
Chapter 7: Resources	49
Support.....	49
Searching a documentation collection.....	50
Subscribing to e-notifications.....	51

Chapter 1: Introduction

Purpose

The Quick Start Guide provides basic instructions to install the hardware and configure the switch.

Chapter 2: New in this release

The following section details what is new in *Quick Start Configuration for Avaya Ethernet Routing Switch 4800 Series*, NN47205-104.

Features

There are no feature-related changes for Release 5.9.

Other changes

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

Quick Start Configuration for Avaya Ethernet Routing Switch 4000 Series is renamed *Quick Start Configuration for Avaya Ethernet Routing Switch 4800 Series*.

Introduction chapter

Information about Related resources and Support are moved to the last chapter in this document.

Chapter 3: Fundamentals

Provisioning follows hardware installation.

The *Quick Start Configuration for Avaya Ethernet Routing Switch 4800 Series*, NN47205-104 includes the minimum, but essential, configuration steps to:

- Provide a default, starting point configuration
- Establish a management interface
- Establish basic security on the node

The shipment includes the following:

- An installation kit
- A foldout poster, *Quick Installation of Avaya Ethernet Routing Switch 4800 Series*, NN47205-302.

For more information about hardware specifications and installation procedures, see *Installing Avaya Ethernet Routing Switch 4800 Series*, NN47205-300.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

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

System connection

Use the console cable to connect the terminal to the switch console port. The console cable and connector must match the console port on the switch (DB-9 or RJ-45, depending on your model). The following are the default communication protocol settings for the console port:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No flow control
- VT100 or VT100/ANSI Terminal Protocol

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
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



Secure and nonsecure protocols

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

Table 2: Secure and nonsecure protocols

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

Table continues...

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
Telnet	Enabled	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 <i>Configuring Security on Avaya Ethernet Routing Switch 4800 Series</i> , NN47205-505.	Disabled
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
 Note: On SSH, by default, HTTP is enabled and HTTPS is disabled.			

Management port

The switch hardware is not equipped with a designated out-of-band (OOB) management port. Use the management port for OOB management when an IP address is assigned to that port. Use the console interface or the in-band switch IP address set from the console terminal through any network port to manage the switch. Before you can use the OOB management, you must first assign an IP address to the device. Use one of the following three methods to configure the management IP address after logging on:

- If the switch is in factory default mode, the install script runs automatically. You are prompted to enter the IP configuration details.
- If the switch is connected to a network, the switch obtains an IP address through bootp or DHCP.
- Run the installation script manually from Privileged EXEC mode. Use the `install` command.

See [Connecting to the switch](#) on page 16 for more information about connecting a terminal to the console port on the switch.

Password encryption

The local passwords for the switch are stored in the configuration file, encrypted with an Avaya proprietary algorithm.

! **Important:**

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

For more information about configuring passwords, see:

Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series, NN47205-102

Configuring Security on Avaya Ethernet Routing Switch 4800 Series, NN47205-505

Enterprise Device Manager

Enterprise Device Manager (EDM) is an embedded graphical user interface (GUI) that you can use to manage and monitor the platform through a standard web browser. EDM is embedded in the switch software, and the switch operates as a web server, so you do not require additional client software. For more information about EDM, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102.

If you want to manage the switch from a centralized location through Configuration and Orchestration Manager (COM) 2.0 and later, Avaya offers optional, product-specific EDM plug-ins for COM that include other features such as centralized syslog, trap viewer, troubleshooting and diagnostic tools. For more information, or to purchase plug-ins, go to www.avaya.com.

Enterprise Device Manager access

To access EDM, open `http://<deviceip>/login.html` or `https://<deviceip>/login.html` from either Microsoft Internet Explorer 8.x or 9.x, or Mozilla Firefox 3.x.

! **Important:**

You must enable the web server from ACLI to enable HTTP access to 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 is enabled by default and allows HTTPS access to the device. Take the appropriate security precautions within the network if you use HTTP.

If you experience issues while connecting to EDM, check the proxy settings. Proxy settings can affect EDM connectivity to the switch. Clear the browser cache, and do not use a proxy when connecting to the device.

Default user name and password

The following table contains the default user name and password that you can use to log on to the switch using EDM. For more information about changing the passwords, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Table 3: EDM default user name and password

User Name	Password
admin	password

Important:

The default passwords and community strings are documented and well known. Avaya strongly recommends that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Device Physical View

When you access EDM, the first panel in the work area displays a switch summary view. The tab behind the summary view is a real-time physical view of the front panel of the device or stack called the Device Physical View.

Objects in the Device Physical View are:

- Stand-alone switch, called a unit
- Switch stack, called a chassis
- Port

From the Device Physical View, you can:

- Determine the hardware operating status
- Select a switch or a port to perform management tasks on specific objects or view fault, configuration, and performance information for specific objects

Click to select an object. The system outlines the object in yellow to indicate that the object is selected.

The conventions on the device view are similar to the actual switch appearance except that LEDs in Device Physical View do not blink. The LEDs and the ports are color-coded to reflect hardware status. Green indicates the port is up and running; red indicates that the port is disabled.

From the menu bar, you can click the **Device Physical View** tab to open the Device Physical View any time during a session.

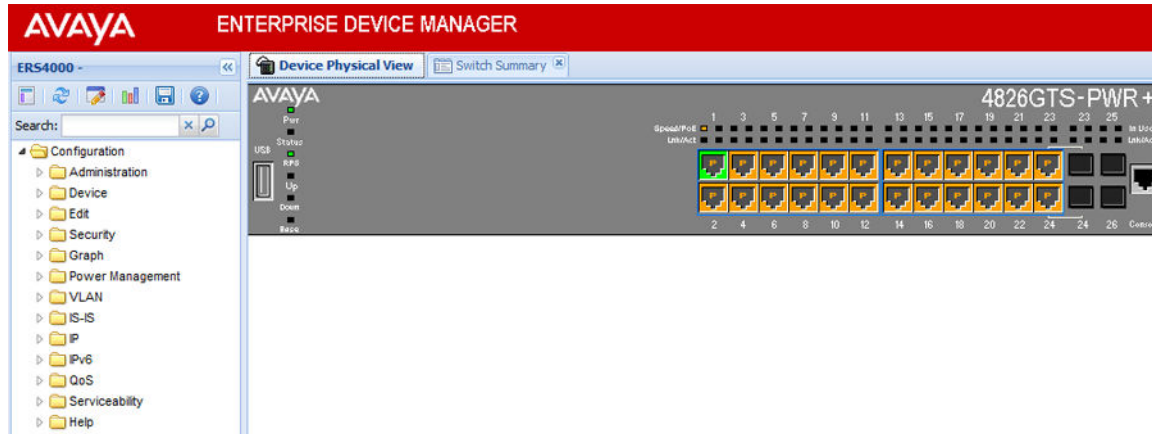


Figure 1: Device Physical View

EDM window

The EDM window contains the following parts:

1. Navigation tree—The navigation pane on the left side of the window that displays available command folders in a tree format.
2. Navigation tree toolbar—The area displays buttons for common functions.
3. Menu bar—The area at the top of the window that displays primary and secondary tabs that you accessed during the session; the tabs remain available until you close them.
4. Toolbar—The area just below the menu bar that provides quick access to the most common operational commands such as **Apply**, **Refresh**, and **Help**.
5. Work area—The main area on the right side of the window that displays the dialog boxes where you view or configure switch parameters.
6. Auto Complete Search — The area between the navigation tree toolbar and the navigation tree where you can type a partial or complete search string to find menus. When you type the search string, the navigation tree changes to display only the entries associated with your search. To return to the full navigation tree display, click the **x** beside the **Auto Complete Search** dialog box.

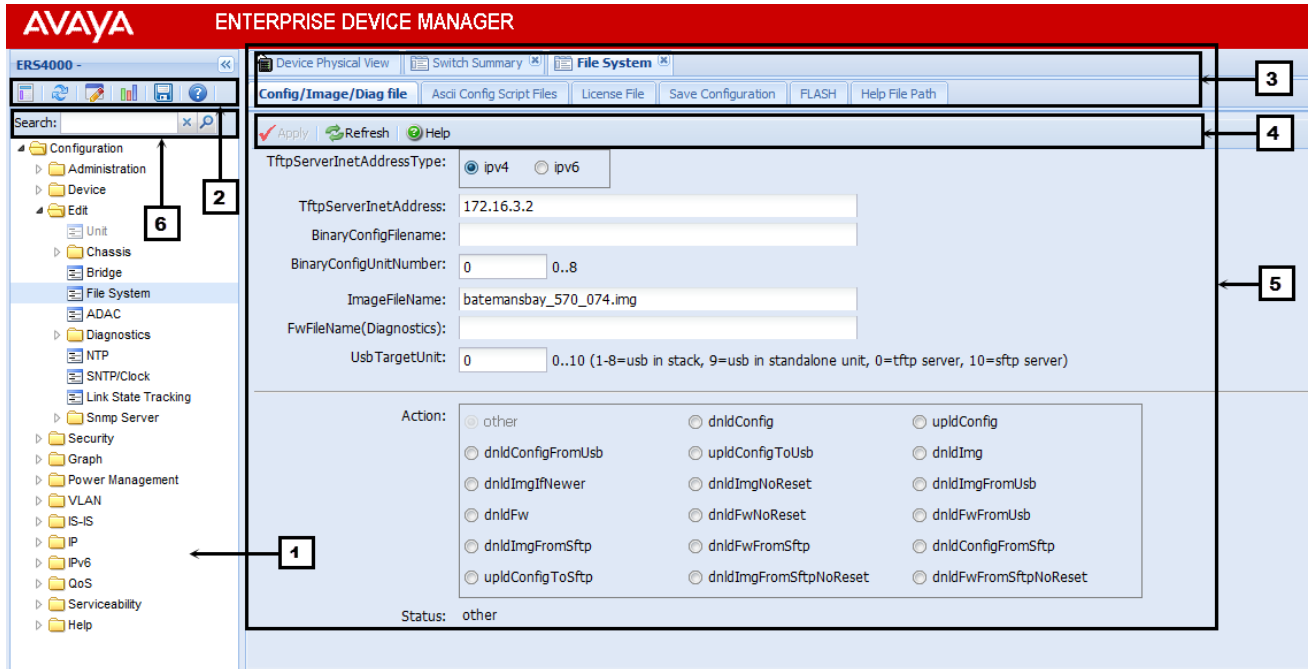


Figure 2: EDM window

Chapter 4: Connecting to the switch

This chapter contains information about how to connect a terminal to the switch and configure the terminal.

Connecting a terminal to the switch

This procedure describes the steps to connect a terminal to the console port on the switch.

Before you begin

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

- Terminal with AC power cord and keyboard. Any terminal or a computer with an appropriate terminal emulator can be used as the management station. See *Installing Avaya Ethernet Routing Switch 4800 Series*, NN47205-300 for a list of the terminal emulation settings that must be used with any terminal emulation software used to connect to the switch.
- Use the RJ-45 or DB-9 console cable to connect the switch console port to your management terminal. See *Installing Avaya Ethernet Routing Switch 4800 Series*, NN47205-300 for console port pin-out information. You can use the pin-out information to verify or create a console cable for use with your maintenance terminal.

Procedure

1. Connect one end of the serial cable to the connector on the terminal or on the computer.
2. Connect the other end of the serial cable to the console port on the switch.
3. Turn the terminal or computer on.
4. Set the terminal protocol on the terminal or terminal emulation program to VT100 or VT100/ANSI.
5. Connect to the switch using the terminal or terminal emulation application. The Avaya switch banner displays when you connect to the switch through the console port.
6. Press `Ctrl+Y` to obtain a CLI prompt.
7. Type the following CLI commands:

```
enable  
install
```

The system displays the setup utility banner.

8. Enter the VLAN ID for the Quick Start at the following prompt:

Please provide the Quick Start VLAN <1-4094> [1]:

9. Enter the IP address at the following prompt:

Please provide the in-band IP Address [0.0.0.0]:

10. Enter the subnet mask at the following prompt:

Please provide the in-band sub-net mask [0.0.0.0]:

11. Enter the default gateway IP address at the following prompt:

Please provide the Default Gateway [0.0.0.0]:

12. Enter the read-only community string at the following prompt:

Please provide the Read-Only Community String [*****]:

13. Confirm the read-only community string at the following prompt:

Please confirm the Read-Only Community String[*****]:

14. Enter the read-write community string at the following prompt:

Please provide the Read-Write Community String [*****]:

15. Confirm the read-write community string at the following prompt:

Please confirm the Read-Write Community String[*****]:

16. Enter the in-band IPv6 address at the following prompt:

Please provide the in-band IPV6 Address/
Prefix_length[1:1:1:1:1:1:1:1/1]:

17. Enter the in-band IPv6 default gateway at the following prompt:

Please provide the in-band IPV6 Default Gateway[::]:

After the procedure is complete, the system displays the following message:

Basic switch parameters have been configured and saved.

Example

```
Welcome to the <Switch> setup utility. You will be requested for information to initially
configure for the switch. When finished the information will be applied and stored in the
switch NVRAM. Once the basic parameters are configured, additional configuration can
proceed using other management interfaces.Press ^C to abort at any time.
Please provide the Quick Start VLAN <1-4094> [1]:1
Please provide the in-band IP Address[0.0.0.0]:10.127.232.30
Please provide the in-band sub-net mask[0.0.0.0]:255.255.255.0
Please provide the Default Gateway[0.0.0.0]:10.127.232.1
Please provide the Read-Only Community String[*****]:*****
Please confirm the Read-Only Community String[*****]:*****
Please provide the Read-Write Community String[*****]:*****
Please confirm the Read-Write Community String[*****]:*****
Please provide the in-band IPV6 Address/Prefix_length[1:1:1:1:1:1:1:1/1]:
Please provide the in-band IPV6 Default Gateway[::]:
Basic switch parameters have now been configured and saved.
```

! Important:

The switch only supports the Avaya CLI. The old Bay Stack menu interface is not supported on this product. When the switch is set to factory default parameters, the CLI Quickstart screen displays, which enables you to configure default IP information.

Configuring the terminal

You can configure the switch terminal settings to suit your preferences for the terminal speed and display.

About this task

Use the following procedure to configure terminal settings including the terminal connection speed, and number of characters in the terminal display width and length.

! Important:

After you modify the terminal configuration, the new settings are applied to the current active session and to all future sessions (serial, telnet or SSH). Terminal configuration change does not affect open concurrent sessions.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
terminal {length <0-132> | width <1-132>}
```
3. To display the current serial port information, enter the following command:

```
show terminal
```

Variable definitions

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

Variable	Definition
length	Set the length of the terminal display in lines. By default, 23 lines are displayed. ! Important: If you set the terminal length to 0, the pagination is disabled and the display scrolls continuously.
width	Set the width of the terminal display in characters. By default, 79 characters are displayed.

Chapter 5: Configuring the switch using CLI

This chapter describes the required procedures for the initial provisioning.

Configuring the management IP address

Use this procedure to configure the IP address and subnet mask for the switch or stack.

Before you begin

Connect the terminal to the switch.

About this task

This procedure configures the switch or stack IP address when the switch configuration is not the factory default.

Important:

When you change the IP address or subnet mask, you can lose connection to telnet and the web. You also disable any new telnet connection, and you must connect to the serial console port to configure a new IP address.

Note:

If you have run the install script to set up the configuration information, the IP address of the device is already configured. If you do not specify the stack or switch parameter when configuring the management IP address, the system automatically modifies the stack IP address when in stack mode and the switch IP address when in standalone mode.

Procedure

1. Press `CTRL+Y` after the Avaya banner displays.
2. Enter Global Configuration mode:

```
enable  
configure terminal
```
3. Assign an IP address to the management port:

```
ip address <A.B.C.D> netmask <A.B.C.D>
```

4. Configure the default gateway IP address:

```
ip default-gateway <A.B.C.D>
```

5. Save the configuration:

```
save config
```

Variable definitions

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

Table 4: ip address command

Variable	Definition
<A.B.C.D>	Set the management IP address.
netmask <A.B.C.D>	Set the subnet mask IP address.

Use the data in the following table to use the `ip default-gateway` command.

Table 5: ip default-gateway command

Variable	Definition
default-gateway <A.B.C.D>	Set the default gateway IP address.

The IP address can range from 0.0.0.0 (no IP address assigned) to 255.255.255.255. For more information about IP addressing and subnet addressing, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.

Configuring BootP on the current instance of the switch or server

About this task

The default operational mode for BootP on the switch is BootP or DefaultIP. The switch requests an IP address from BootP only if one is not already configured from the console terminal (or if the IP address is the default IP address 192.168.1.1).

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
ip bootp server {always | disable | last | default-ip}
```

Variable definitions

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

Variable	Definition
always disable last default-ip	Specify when to use BootP: <ul style="list-style-type: none"> • default-ip—Use BootP or the default IP • last—Use BootP or the last known address • disable—Never use BootP • always—Always use BootP By default, default-ip is selected.

Setting user access limitations

The administrator can use ACLI to limit user access by creating and maintaining passwords for web, telnet, and console access. This is a two-step process that requires that you first create the password and then enable it.

Ensure that you enter Global Configuration mode in ACLI before you start these tasks.

Setting the read-only and read/write passwords

To require password authentication when a user logs in to a switch, you must edit the password configuration.

About this task

Follow this procedure to edit the password configuration.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enter the following command:

```
cli password {read-only | read-write} <password>
```

3. Press Enter.

Variable definitions

The following table describes the parameters for the `cli password` command.

Variable	Definition
{read-only read-write}	Specify whether the password change is for read-only access or read-write access.
<password>	Specify password length. If password security is disabled, the password length can be 1 to 15 characters. If password security is enabled, the range for the password length is 10 to 15 characters.

Enabling and disabling passwords

After you set the read-only and read-write passwords, you can individually enable or disable them for the various switch-access methods.

About this task

Follow this procedure to enable or disable a password for a specific access method.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
cli password {telnet | serial} {none | local | radius | tacacs}
```

3. Press `Enter`.

Variable definitions

The following table describes the variables for the `cli password` command.

Variable	Definition
{telnet serial}	Specify whether the password is enabled or disabled for telnet or the console. Telnet and web access are connected so that enabling or disabling passwords for one enables or disables passwords for the other.
none local radius tacacs	Specify the password type to modify: <ul style="list-style-type: none"> • none: disables the password. • local: uses the locally defined password for serial console or telnet access.

Table continues...

Variable	Definition
	<ul style="list-style-type: none"> • radius: uses RADIUS authentication for serial console or telnet access. • tacacs: uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or telnet access.

Setting user access limitations using Enterprise Device Manager

You can use Enterprise Device Manager (EDM) to limit user access by creating and maintaining passwords for web, telnet, and console access.

Configuring the console password using EDM

About this task

Use this procedure to configure a password for serial console access to a stack or standalone switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Web/Telnet/Console**.
3. In the work area, click the **Console Password** tab.
4. Click the arrow on the **Console Stack Password Type** field.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Stack Password** field.
7. Type the same password for read-only access in the **Re-enter to verify** field.
8. Type the password for read-write access in the **Read-Write Stack Password** field.
9. Type the same password for read-write access in the **Re-enter to verify** field.
10. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to configure the console switch password.

Variable	Definition
Console Stack Password Type	Specify the type of password to use. Values include: <ul style="list-style-type: none"> • none—Disables the password • Local Password—Use the locally-defined password for serial console access. • RADIUS Authentication—Use RADIUS authentication for serial console access. • TACACS Authentication—Use TACACS+ authentication, authorization, and accounting (AAA) services authentication for console access.
Read-Only Stack Password	Specify the read-only password for stack or switch access.
Read-Write Stack Password	Specify the read-write password for stack or switch access.

Configuring the web and telnet password using EDM

About this task

Use the following procedure to configure a password for web and telnet access to a stack or standalone switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Web/Telnet/Console**.
3. In the work area, click the **Web/Telnet** tab.
4. Click the arrow on the **Web/Telnet Switch Password Type** field.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Stack Password** field.
7. Type the same password for read-only access in the **Re-enter to verify** field.
8. Type the password for read-write access in the **Read-Write Switch Password** field.
9. Type the same password for read-write access in the **Re-enter to verify** field.
10. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to configure the web and telnet switch password.

Variable	Definition
Web/Telnet Stack Password Type	Specify the type of the password to use. Values include: <ul style="list-style-type: none"> • none—Disables the password • Local Password—Uses the locally defined password for web and telnet access. • RADIUS Authentication—Uses RADIUS password authentication for web and telnet access. • TACACS Authentication—Uses TACACS+ authentication, authorization, and accounting (AAA) services authentication for web and telnet access.
Read-Only Stack Password	Specify the read-only password for stack or switch access. The maximum length of the password is 15 characters.
Read-Write Switch Password	Specify the read-write password for stack or switch access. The maximum length of the password is 15 characters.

Configuring the ACLI banner

You can configure the banner that is presented when a user logs on to the switch through ACLI to a user-defined value.

You can use the custom logon banner to display company information, such as company name and contact information.

The banner cannot exceed 1539 bytes, or 19 rows by 80 columns plus line termination characters. The banner control setting is saved to NVRAM, and both the banner file and control setting are distributed to all units within a stack.

About this task

Follow this procedure to configure the ACLI banner.

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:

Configuring the switch using ACLI

```
banner <line_number> "<LINE>"
```

4. Save the configuration:

```
save config
```

5. Display the banner information:

```
show banner
```

6. Log on again to verify the configuration.

7. (Optional) Disable the banner:

```
no banner
```

Example

The following is an example of ACLI banner configuration:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#show banner
Current banner setting: STATIC
Switch(config)#banner custom
Switch(config)#banner 1 "My Company Name"
Switch(config)#banner 2 "123A My Address Avenue      My Town  CA 12345"
Switch(config)#banner 3 "Phone: (123) 555-5555 * Fax (123) 555-5555"
Switch(config)#banner 4 "http://www.mycompanywebsite.com"
Switch(config)#save config
Switch(config)#show banner
Current banner setting: CUSTOM
Switch(config)#end
Switch#exit
My Company Name
123A My Address Avenue      My Town  CA 12345
Phone: (123) 555-5555 * Fax (123) 555-5555
http://www.mycompanywebsite.com
```

Enter Ctrl-Y to begin.

```
*****
*** Ethernet Routing Switch <Switch>
*** Avaya
*** Copyright (c) 1996-2014, All Rights Res
***
*** HW:ROA2      FW:5.9.0.1  SW:v5.9.0.145
*****
```

Variable definitions

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

Variable	Definition
custom	Disable the use of the default banner.
static	Activate the use of the default banner.
<line_number>	Banner line number you are configuring. The range is 1 to 19
<LINE>	Specify the characters in the line number.

Configuring system identification

About this task

You can configure system identification to specify the system name, contact person, and location of the switch, and to add a trap receiver to the trap-receiver table.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable the Simple Network Management Protocol (SNMP) server:

```
snmp-server enable
```

3. Configure the read-only community name:

```
snmp-server community ro
```

*** Note:**

Enter the community string twice.

If you ran the install script to set up the configuration information, the read-only community name is already configured.

4. Configure the read-write community name:

```
snmp-server community rw
```

*** Note:**

Enter the community string twice.

If you ran the install script to set up the configuration information, the read-write community name is already configured.

5. Configure the system name:

```
snmp-server name "<text>"
```

6. Configure the system contact:

```
snmp-server contact "<text>"
```

7. Configure the location:

```
snmp-server location "<text>"
```


8. Configure the SNMP host to add a trap receiver to the trap-receiver table:

```
snmp-server host <host-ip> <community-string>
```

Variable definitions

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

Table 6: snmp-server name command

Variable	Definition
<text>	Specify the SNMP system name value. Enter an alphanumeric string of up to 255 characters.  Note: On the console, the SNMP server name is truncated. On the web interface, the full SNMP server name appears.

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

Table 7: snmp-server contact command

Variable	Definition
<text>	Specify the SNMP system contact value. Enter an ASCII string of up to 255 characters.

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

Table 8: snmp-server location command

Variable	Definition
<text>	Specify the SNMP system location value. Enter an alphanumeric string of up to 255 characters.

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

Table 9: snmp-server host command

Variable	Definition
<code><host-ip></code>	Specify an IPv4 or IPv6 address for a host intended to be the trap destination.
<code><community-string></code>	If you are using the proprietary method for SNMP, enter a community string that works as a password and permits access to the SNMP protocol.

Enabling logging

Use this procedure to enable the logging of system messages. For more information about logging, see *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. To enable system logging, enter the following command at the command prompt:


```
logging remote level informational
```

Configuring Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) feature synchronizes the Universal Coordinated Time (UTC) to an accuracy within 1 second. This feature adheres to the IEEE RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030-compliant NTP/SNTP server.

For more information on SNTP, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205–500.

About this task

Use this procedure to configure the Network Time Protocol (NTP) servers for SNTP.

Procedure

1. Enter Global Configuration mode:


```
enable
```

```
configure terminal
```

2. Enter the following command to configure the SNTP server primary IP address:

```
sntp server primary address [<A.B.C.D> |  
<primary_server_ipv6address>]
```

3. Enter the following command to configure the SNTP secondary server IP address:

```
sntp server secondary address [<A.B.C.D> |  
<secondary_server_ipv6address>]
```

*** Note:**

SNTP supports primary and secondary NTP servers. The system attempts to access the secondary NTP server only if the primary NTP server is unresponsive.

4. Enter the following command to enable SNTP:

```
sntp enable
```

Variable definitions

The following table describes the parameters for the `sntp server` command.

Variable	Definition
<A.B.C.D>	Enter the IP address of the NTP server.
<primary_server_ipv6address>	Enter the IPv6 address of the primary NTP server.
<secondary_server_ipv6address>	Enter the IPv6 address of the secondary NTP server.

Configuring local time zone

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data does not include daylight saving time changes. You must configure daylight saving time.

About this task

Use this procedure to configure the local time zone.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enter the following command to enable SNTP:

```
sntp enable
```

3. Enter the following command to configure the time zone:

```
clock time-zone zone hours [minutes]
```

4. Enter the following command to configure daylight saving time:

```
clock summer-time zone date day month year hh:mm day month year
hh:mm [offset]
```

5. Save the changed configuration.

Example

Configuring the time zone

```
Switch>enable
Switch#configure terminal
Switch(config)#clock time-zone PST -8
```

Configuring daylight saving time

This command sets the time zone to UTP minus 8 hours and the time zone is displayed as "PST."

```
Switch(config)#clock summer-time BST date 28 Mar 2013 2:00 30 Aug 2013 15:00 +60
```

This command sets the daylight saving time to begin at 02:00 on March 28, 2013 and end on August 30, 2013 at 15:00. The change to daylight saving time moves the clock forward by 60 minutes and the time zone is displayed as "BST". These changes to and from daylight saving time occur automatically.

Variable definitions

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

Table 10: clock time-zone command

Variable	Definition
zone	Time zone acronym to be displayed when showing system time (up to 4 characters).
hours	Difference from UTC in hours. This can be any value between -12 and +12.
minutes	Optional: This is the number of minutes difference from UTC. Minutes can be any value between 0 and 59.

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

Table 11: clock summer-time zone command

Variable	Definition
date	Indicates that daylight saving time you set to start and end on the specified days every year.

Table continues...

Variable	Definition
day	Day to start daylight saving time.
month	Month to start daylight saving time.
year	Year to start daylight saving time.
hh:mm	Hour and minute to start daylight saving time.
day	Day to end daylight saving time.
month	Month to end daylight saving time.
year	Year to end daylight saving time.
hh:mm	Hour and minute to end daylight saving time.
offset	Number of minutes to add during the summertime.
zone	The time zone acronym to be displayed when daylight saving time is in effect. If unspecified, the acronym defaults to the time zone acronym that was configured when the time zone was configured.

Configuring the clock

In addition to SNTP time configuration, a clock provides the switch with time information. This clock provides the switch information when SNTP time is not available.

About this task

Use this procedure to configure the time source for the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
clock source {ntp | sntp | sysUpTime }
```

Variable definitions

The following table describes the parameters for the `clock source` command.

Variable	Definition
ntp	Configure NTP as the time source.
sntp	Configure SNTP as the time source.
sysUpTime	Configure System Up Time as the time source.

Configuring a static route

Create static routes to manually configure a path to destination IP address prefixes.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command to enable IP routing globally:

```
ip routing
```

3. Enter the following command to configure an IP address on a VLAN:

```
ip address <ip address> <mask> [<MAC-offset>]
```

4. Enter the following command to configure a static route:

```
ip route <destination ip> <mask> <next-hop> {<cost> | disable |
enable | weight <cost>}
```

5. Enter the following command to display all the static routes:

```
show ip route static [<dest-ip>] [-s <subnet> <mask>]
```

6. Save the configuration.

Variable definitions

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

Variable	Definition
<ipaddr>	Specify the IP address to attach to the VLAN.
<mask>	Specify the subnet mask to attach to the VLAN
<MAC-offset>	Specify the value used to calculate the VLAN MAC address, which is offset from the switch MAC address. The valid range is 1 to 256. Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.
<destination ip>	Specify the destination IP address for the route being added. 0.0.0.0 is considered the default route.
<mask>	Specify the destination subnet mask for the route being added.

Table continues...

Variable	Definition
<next-hop>	Specify the next-hop IP address for the route being added.
<cost>	Specify the weight, or cost, of the route being added. Range is 1 to 65535.
enable	Enable the specified static route.
disable	Disable the specified static route.
weight <cost>	Change the weight, or cost, of an existing static route. Range is 1 to 65535.

Enabling remote access

You can enable remote access for telnet, SSH (on SSH software images), SNMP, and webpage access.

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102 and *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.

About this task

Use the following procedure to enable and configure remote access to the management features of the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To enable telnet remote access, enter the following command:

```
telnet-access enable
```

3. To enable SSH remote access, enter the following command:

```
ssh
```

4. To enable SNMP remote access, enter the following command:

```
snmp-server enable
```

5. To enable webpage remote access, enter the following command:

```
web-server enable
```

Example

The following is an example of enabling telnet remote access:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#telnet-access enable
Switch(config)#
```

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 computer or terminal, start a telnet session:

```
telnet <IPv4_address>
```

where <IPv4_address> is the IP address of the switch. The stand-alone units use the default IP address of 192.168.1.1 if the switch does not obtain its IP address from another source.

2. Enter the user ID and password when prompted.

Enabling the web server management interface

The web server must be enabled to access Enterprise Device manager (EDM). If you do not want EDM to be accessible on the device, disable the web server. By default, the web server is enabled.

About this task

Use this procedure to enable the web server.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
web-server enable
```

Accessing the switch through the web interface

You can use EDM to configure and maintain your switch through a web-based graphical user interface. You can monitor the switch through a web browser from anywhere on the network.

By default, you can access the web interface using Hypertext Transfer Protocol Secure (HTTPS) only.

For more information about configuring the web server to respond to HTTPS only or to both HTTPS and Hypertext Transfer Protocol (HTTP) client browser requests, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

By default, the web interface uses a 15 minute time-out period. If no activity occurs for 15 minutes, the system logs off the switch web interface, and you must reenter the password information.

To configure inactivity time-out, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Before you begin

- Ensure that the switch is running.
- Note the switch IP address.
- Ensure that the web server is enabled.
- Note the user name and password.
- Open one of the supported web browsers.

For more information about the supported browsers, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102

About this task

Use this procedure to access the switch through a web browser.

Procedure

1. Start your web browser.
2. Type the switch IP address as the URL in the Web address field.

```
http://<IP Address>
```

OR

```
https://<IP Address>
```

3. Enter the user name.
4. Enter the password.
5. Click **Log On**.

Configuring a VLAN

Use this procedure to create a VLAN using ACLI. Optionally, you can choose to assign the VLAN a name or rename the VLAN.

For more information about configuring a VLAN, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command at the command prompt:

```
vlan create <VID_list> [name <LINE>] type { port { voice-vlan |
remote-span | [<1-8>] { voice-vlan | remote-span } } | protocol
decEther2 | protocol-ipEther2 | protocol-ipv6Ether2 | protocol
ipx802.2 | protocol-ipx802.3 | protocol-ipxEther2 | protocol ipxSnap
| protocol-Netbios | protocol-RarpEther2 | protocol sna802.2 |
protocol-snaEther2 | protocol-vinesEther2 | protocol-xnsEther2 |
protocol-Userdef {ether <4096-65534> | llc <1-65534> | snap
<1-65534>} | voice-vlan | spbm-bvlan | spbm-switchedUni [<1-8>]} |
[voice-vlan]
```

* Note:

If you tag protocol VLAN client ports, the system cannot assign frames to the protocol VLAN, regardless of the defined ethertype. Frames are not assigned to the protocol VLAN because untagged packets are assigned to the VLAN identified by the port PVID.

Example

Creating a range of port-based VLANs:

```
Switch(config)#vlan create 100,107,109-113,115 type port
```

Creating a protocol-based VLAN:

```
Switch(config)#vlan create 200 type protocol-decEther2
```

Creating and naming a voice-VLAN:

```
Switch(config)#vlan create 300 name my_vlan type port voice-vlan
```

Renaming an existing VLAN:

```
Switch(config)#vlan name 300 my_vlan2
```

Creating a VLAN using a user-defined protocol and specifying the frame encapsulation header type:

```
Switch(config)#vlan create 500 type protocol-userdef ether 6004
```

Creating an SPBM-BVLAN:

```
Switch(config)#vlan create 600 type spbm-bvlan
```

Creating an RSPAN VLAN:

```
Switch(config)#vlan create 700 type port remote-span
```

Displaying a range of VLANs:

```
Switch(config)#show vlan id 100,107,109-113,115,200,300,500,600,700
Id   Name                               Type      Protocol      PID      Active  IVL/SVL  Mgmt
-----
100  VLAN #100                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
107  VLAN #107                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
109  VLAN #109                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
110  VLAN #110                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
111  VLAN #111                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
112  VLAN #112                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
113  VLAN #113                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
115  VLAN #115                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
200  VLAN #200                          Protocol  Declat Ether2  0x6004   Yes     IVL       No
      Port Members: NONE
300  my_vlan2                          Voice     None          0x0000   Yes     IVL       No
      Port Members: NONE
500  VLAN #500                          Protocol  Ether2 User-Def.  0x1774   Yes     IVL       No
      Port Members: NONE
600  VLAN #600                          B-VLAN   None          0x0000   Yes     IVL       No
      Port Members: NONE
700  VLAN #700                          Port      None          0x0000   Yes     IVL       No
      Port Members: NONE
Total VLANs: 13
```

Variable definitions

The following table describes the parameters for the `vlan create` command.



Variable	Definition
<VID_list>	Enter as an individual VLAN ID to create a single VLAN or enter as a range of VLAN IDs to create multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094.  Note: VLAN ID values 4001 through 4008 are reserved and cannot be used.
name <line>	Specify a unique alphanumeric name for an individual VLAN.

Table continues...

Variable	Definition
	<p> Note:</p> <p>Do not enter a value for this parameter when you are creating multiple VLANs simultaneously.</p>
type	<p>Enter the type of VLAN to create:</p> <ul style="list-style-type: none"> • port—Port-based • protocol—Protocol-based (see the following list)
remote-span	Specify as RSPAN VLAN.
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-RarpEther2	Specify a RarpEther2 protocol-based VLAN.
protocol-sna802.2	Specify an sna802.2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.
protocol-Userdef	<p>Specify a user-defined protocol-based VLAN.</p> <p>Enter</p> <ul style="list-style-type: none"> • <code><4094-65534> {<1-8> voice-vlan}</code>—Ethernet II user-defined VLAN with this Protocol ID, where <1-8> is Spanning Tree Group ID • <code>ether <4096-65534></code>—Ethernet II user-defined VLAN with this Protocol ID • <code>llc <1-65534></code>—LLC user-defined VLAN with this Protocol ID • <code>snap <1-65534></code>—SNAP user-defined VLAN with this Protocol ID
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
<1-8>	Specify the Spanning Tree Group ID.
spbm-bvlan	Specify as SPBM B-VLAN.
spbm-switchedUni	Specify as SPBM switched UNI.
voice-vlan	Specify as Voice VLAN.

Configuring VLAN using EDM

You can create a VLAN by IP subnet, port, protocol, or source MAC address using EDM.

You can 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 the switch. For more information about the VLAN configuration rules and about configuring a VLAN, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.

About this task

Use this procedure to create a VLAN and assign an IP address to a VLAN to enable routing on the VLAN.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > VLAN**.
2. Click **VLANs**.
3. On the **Basic** tab, click **Insert**.
4. In the **Id** field, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** field, type the VLAN name, or use the name provided.
6. In the **StgId** field, specify the IDs to associate STG with the selected VLAN or VLANs.
7. In the **Type** box, select the type of VLAN you want to create.
 - To create a VLAN by port, select **byPort**.
 - To create a VLAN by protocol, select **byProtocolId**. This activates additional fields to configure protocol-based VLANs, including a selection of various protocols.
 - To associate a Shortest Path Bridging–MAC (SPBM) network instance with one backbone VLAN in the core SPBM network, select **spbm-bvlan**.
 - To use VLAN and create an endpoint to one Service Instance VLAN ID (I-SID) and another port to create an endpoint to another I-SID, select **spbm-switchedUni**.
8. Select **VoiceEnabled** to indicate whether a VLAN is voice VLAN.
9. Select **RspanEnabled** to indicate whether a VLAN is RSPAN enabled.

Variable definitions

Use the data in the following table to create a VLAN using EDM.


Variable	Definition
Id	Specify the ID for the VLAN.
Name	Specify an alphanumeric name for the VLAN. If you do not type a name, the switch default name is applied.
StgId	Specify the Spanning Tree Group (STG) to associate with the selected VLAN or VLANs. This is a read-only value.  Important: This column is available only when the Spanning Tree administration operating mode is avayaSTG mode. When the operating mode is Multiple Spanning Tree Protocol (MSTP) or Rapid Spanning Tree Protocol (RSTP), this column is not available.
Type	Indicate the type of VLAN. This is a read-only value. Values include: <ul style="list-style-type: none"> • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID • spbm-bvlan—Backbone VLAN for the Shortest Path Bridging MAC (SPBM) • spbm-switchedUni—To create one endpoint on one Service Instance ID (I-SID) and another endpoint on another I-SID.
VoiceEnabled	Indicate whether VLAN is a voice VLAN (true) or not (false).
RspanEnabled	Indicate whether VLAN is an RSPAN VLAN (true) or not (false).
ProtocolId	Indicate the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId. Values include: <ul style="list-style-type: none"> • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2

Table continues...

Variable	Definition
	<ul style="list-style-type: none"> • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp

Installing a license file

Use this procedure to install a license file.

If the switch is reset to default, the license file must be reinstalled to reenble licensed features. Resetting a switch to default removes the license file from its storage area in NVRAM. Store the license file on a TFTP server accessible by the switch or stack before starting the installation procedure. For switches equipped with a USB port, you can also use a USB mass storage device to copy the license file to the switch.

About this task

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
copy [tftp | usb] license <tftp_ip_address> filename
<license_file_name>
```

3. Restart the switch.

Example

Installing a license using USB

1. Insert a USB mass storage device into a USB port on the front of the switch.
2. To copy a license from a USB mass storage device, use the following commands:

```
Switch>enable
Switch#copy usb license 4000_adv.lic
```

The switch generates the following message:

```
License successfully downloaded.
```

! **Important:**

You must restart the system to activate the license.

Saving the configuration

After you change the configuration, you must save the changes. Save the configuration to a file to retain the configuration settings.

***** **Note:**

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

Before you begin

Enable the Trivial File Transfer Protocol (TFTP) on the switch.

About this task

Use this procedure to save the configuration.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
save config
```

Storing the configuration files

Before and after you upgrade your switch software, make copies of the configuration files. If an error occurs, use backup configuration files to return to a previous state. You can store the files in binary or ASCII format. Use the following procedure to store the configuration file in binary format. For more information about storing the file in ASCII format, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Avaya recommends that you keep several copies of backup 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. FTP and TFTP support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

About this task

Use this procedure to copy the saved configuration to a file in binary format.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
copy config usb {filename <filename> | unit <1-8>
```

Variable definitions

Use the data in the following table to use the `copy config usb` command.

Variable	Definition
<filename>	The name of the file to be retrieved.
<1-8>	The unit number in which the USB device is inserted, if the unit is a part of the stack.

Shutting down the switch

The switch administrator can use this feature to safely shut down the switch without interrupting a process or corrupting the software image. After you issue the command, the configuration is saved, auto-save functionality is temporarily disabled, and you are notified that it is safe to power off the switch. If you cancel the shutdown, auto-save functionality returns to the state in which it was previously functioning.

Important:

Any configurations or login performed on the switch after you initiate the shutdown command are not saved to NVRAM and are lost after the reset.

About this task

Use this procedure to shut down the switch.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
shutdown [force][minutes-to-wait <1-60>] [cancel]
```

Variable definitions

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

Variable	Definition
force	Instruct the switch to skip the shutdown confirmation prompt.
minutes-to-wait <1-60>	Specify the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancel all scheduled switch shutdowns.

Reloading a remote switch after configuration

This procedure is intended to be used by system administrators to reload a remote switch when configuration is complete. The configuration is not explicitly saved after the `reload` command is issued. This means that any configuration changes must be explicitly saved before the switch reloads.

Use this procedure to disable auto-saving configuration changes and safeguard against a configuration error when you perform dynamic configuration changes on a remote switch. If you make an error while configuring a remote switch that results in the loss of connectivity (for example, an error in the IP address or VLAN), the reload loads the last saved configuration to re-establish connectivity.

This procedure temporarily disables auto-save functionality until the reload occurs. If you cancel the reload, auto-save functionality returns to any previous setting.

Caution:

You must perform a timed reload command before making dynamic configuration changes to safeguard against the loss of remote connectivity.

About this task

Use this procedure to reload a remote switch.

Procedure

1. Enter Privileged EXEC mode:


```
enable
```
2. At the command prompt, enter the following command:


```
reload [force] [minutes-to-wait] [cancel]
```

Variable definitions

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

Variable	Definition
force	Instruct the switch to skip the shutdown confirmation prompt.
minutes-to-wait <1-60>	Specify the number of minutes before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancel all scheduled switch shutdowns.

Chapter 6: Verification

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

Pinging an IP device

You can ping a device to test the connection between Ethernet Routing Switch 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, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address does not respond.

About this task

Use this procedure to ping a device.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
ping <IP_address>
```

where <IP_address> is an IPv4 or IPv6 address.

Verifying the software release

About this task

Use this procedure to display the currently-loaded and operational software load

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show boot [diag] [image]
```

Variable definitions

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

Variable	Definition
diag	Display only information for the agent load.
image	Display only information for the image load.

Important:

When the currently loaded and operational software status is displayed for a stack, the unit number is replaced by the word **All**.

Displaying local alarms

You can 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 and 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.

About this task

Use this procedure to display local alarms.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command :

```
show rmon alarm
```


Chapter 7: Resources

Support

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

Documentation

For a list of the documentation for this product and more information about documents on how to configure other switch features, see *Documentation Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205–101.

For more information on new features of the switch and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 4800 Series*, NN47205-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

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

Training

Ongoing product training is available. For more information or to register, see <http://avaya-learning.com/>.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

Searching a documentation collection

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

Before you begin

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

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named `<product_name_release>.pdx`.

3. In the Search dialog box, select the option **In the index named <product_name_release>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
 - Whole Words Only
 - Case-Sensitive
 - Include Bookmarks
 - Include Comments
6. Click **Search**.

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

Subscribing to e-notifications

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

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

GENERAL NOTIFICATIONS
1/5 Notifications Selected

End of Sale and/or Manufacturer Support Notices	<input type="checkbox"/>
Product Correction Notices (PCN)	<input checked="" type="checkbox"/>
Product Support Notices	<input type="checkbox"/>
Security Advisories	<input type="checkbox"/>
Services Support Notices	<input type="checkbox"/>

UPDATE >>

6. Click **OK**.
7. In the **PRODUCT NOTIFICATIONS** area, click **Add More Products**.

PRODUCT NOTIFICATIONS [Add More Products](#)

Show Details **1 Notices**

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.

PRODUCTS	My Notifications
Virtual Services Platform 7000	VIRTUAL SERVICES PLATFORM 7000 Select a Release Version All and Future
Virtualization Provisioning Service	
Visual Messenger™ for OCTEL® 250/350	
Visual Vectors	
Visualization Performance and Fault Manager	
Voice Portal	
Voice over IP Monitoring	
W310 Wireless LAN Gateway	
WLAN 2200 Series	
WLAN Handset 2200 Series	
	Administration and System Programming <input type="checkbox"/> Application Developer Information <input type="checkbox"/> Application Notes <input type="checkbox"/> Application and Technical Notes <input checked="" type="checkbox"/> Declarations of Conformity <input type="checkbox"/> Documentation Library <input checked="" type="checkbox"/>
	SUBMIT >>

11. Click **Submit**.