Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series

Release 5.10
NN47205-102
Issue 09.01
September 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 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, 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.

Service Provider

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

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

Compliance with Laws

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,

Contents

Chapter 1: Introduction

Purpose

This document provides information about the Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM) for the switch.

Chapter 2: New in this document

The following sections detail what is new in *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102 for Release 5.10.

ACLI pipe filter commands

Pipe filter commands can be added to existing ACLI commands. The ACLI command is followed by the pipe (|) symbol then the pipe filter command. The ACLI command output is filtered and contains only the lines specified in the pipe filter.

For more information, see the following sections:

- ACLI Pipe filter on page 21.
- ACLI pipe filter functions on page 57.

Ability to query USB file information

General file information on a USB flash device can be viewed in Enterprise Device Manager. For more information, see Displaying USB File Information on page 53.

Chapter 3: Feature licensing fundamentals

This chapter provides information to help understand, install, and manage feature licensing. Review this chapter before using licensed features or before making changes to the license configuration.

❗ **Important:**

If you reset a standalone device to the default configuration, you erase the license file.

Feature licenses

This section describes the types of licenses and lists the features that require a license. Software releases prior to Release 5.4 require no licenses. Switches and licenses are purchased separately. Trial and advanced license types are supported.

To use the following features you must obtain the appropriate license:

- Open Shortest Path First (OSPF) (beginning with Release 5.4)
- Virtual Router Redundancy Protocol (VRRP) (beginning with Release 5.5)
- Equal Cost Multi Path (ECMP) (beginning with Release 5.6)
- Protocol Independent Multicast-Sparse mode (PIM-SM) (beginning with Release 5.8)

You can obtain a trial license to try out advanced license features for 30 days. Trial licenses are obtained from Avaya and installed using the ACLI. After the trial period expires, the licensed feature is disabled.

To minimize network and device impacts, the following events occur before the expiration of a trial license:

- A system trap is sent five days before license expiration.
- A system trap is sent one day before license expiration.
- A system trap is sent at license expiration.

To fully enable advanced license features, you must purchase a license kit, generate a license file, and install the file on the switch. Each license kit contains a license certificate and a License Authorization Code (LAC) for a specific number or level of licenses. The license certificate contains the following instructions for license file generation:

- Obtain the switch Base MAC address for license file generation.
- Go to www.avayadatalicensing.com, enter user information, and select the required action. For example, select **Create/Generate a License file for your Avaya data product**.

Note:

An email address is mandatory so that the license file can be forwarded for installation on your Avaya switch.

- Enter the License Authorization Code (LAC) to receive license entitlements and generate a license file.
- Install the license file on the switch.

License generation

After you purchase a license kit, you must generate a license file using the Avaya data licensing portal. The licensing portal is where license files are generated or MAC addresses are swapped in existing license files.

The license certificate found in the license kit contains a License Authorization Code (LAC). This LAC is submitted to the license portal, which deposits license entitlements into a license bank. This license entitlement is combined with the switch MAC address to generate a license file. Because license files are generated based on a switch MAC address, the license file must contain the authorized MAC addresses of the switches where it will be installed.

A license can contain multiple MAC addresses and MAC addresses can be added to the license file at a later time. A single license file can support more than one MAC address. The number of MAC addresses supported is dependent on the type of license. To support licensed features in a stack, use the MAC address of the Base Unit.

The following table provides information on the license kits available for the switch.

Product Order Code	License Type	Number of switches / switch stacks supported
AL4516001	ERS4000 Adv License	1
AL4516002	ERS4000 Adv License	10

Generating a license file

This section describes the procedure for license file generation.

Before you begin

Ensure the following prerequisites are met before generating a license:

- Purchase a license kit.
- Ensure a properly-configured TFTP server is reachable from the switch or stack on which the license file will be installed.
- Obtain the switch base MAC addresses for the switches that use licensed features.

License file names must conform to the following limitations:

- 63 character maximum.
- Lowercase characters only.
- No spaces or special characters permitted with the exception of the underscore (_).
- A three-character file extension is required. This file extension can be any three characters.

To generate a license file for multiple MAC addresses, you must specify the addresses in a text file that conforms to the following rules:

- ASCII text file.
- One MAC address per line.
- No additional characters, spaces, or special characters besides those used in the MAC addresses.
- MAC addresses in hexadecimal, capitalized format with each pair of characters separated by colons.
- Must contain correct MAC addresses.
- The number of MAC addresses specified must not exceed the maximum for the license type.

About this task

Follow this procedure to generate a license file.

Procedure

1. Use a web browser to access the licensing portal.
2. Enter the contact information in the required boxes. It is mandatory to enter an email address.
3. Select **Create/Generate a License file for your Avaya data product**.
4. Enter the License Authorization Code.
5. Enter switch or switch stack base MAC address(es). If the LAC is for 10 or more license entitlements, enter multiple MACs to be embedded in the license file.
6. Specify the License Bank name (optional).
7. Specify the License file name (optional).

   You can rename a license file before it is installed on a switch.
8. Click **Submit Request**.

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 reenable 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 filename 4000_adv.lic
   ```

   The switch generates the following message:

   ```
   License successfully downloaded.
   ```

Important:

You must restart the system to activate the license.

Installing a license file using SFTP

Before you begin

- Store the license file on an SFTP server accessible by the switch or stack before starting the installation procedure.
- For authentication using an RSA or Digital Signature Algorithm (DSA) key, the authentication key must be generated and uploaded to the SFTP server.

About this task

Follow this procedure to install a license file using SFTP.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Use the following command to download and install the license file if you use an RSA or DSA key for authentication.

   ```
   copy sftp license address <sftp_ip_address> filename
   <license_file_name> username <user_name>
   ```

3. Use the following command to download and install the license file if you use a password for authentication.

   ```
   copy sftp license address <sftp_ip_address> filename
   <license_file_name> username <user_name> password
   ```

4. Restart the switch.

Variable definitions

The following table describes the parameters for the `copy sftp license` command.

Variable	Definition
<sftp_ip_address>	Specifies the address of the SFTP server.
<license_file_name>	Specifies the license file name.
<user_name>	Specifies the user name.

Displaying licenses

About this task

Follow this procedure to display installed license files

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command.

   ```
   show license {<1-10> | all} [verbose]
   ```

   Specify an individual license with the designated number or use the `all` keyword to display all installed licenses.

Deleting a license

About this task

Follow this procedure to delete an installed license.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command.

   ```
   clear license { <1-10> | all}
   ```

   Specify an individual license with the designated number or use the `all` keyword to delete all installed licenses.

Transferring a license

The switch implements Licensing Auto Unit Replacement. If a base unit fails, the other units in the stack transfer a virtual key to the new base unit to eliminate the need for transfer of a license to the new base unit. Even with this functionality in place, there are still several situations where it becomes necessary to transfer the license from one device to another. These conditions are as follows:

- Replacement of failed non-base unit.
- Incorrect MAC address entered during license file generation.
- The system displays an error message indicating the limit of MAC swaps for the license has been exceeded.

About this task

Use the following procedure to transfer a license.

Procedure

1. Use a web browser to access the licensing portal.
2. Enter the contact information in the required boxes.

   It is mandatory to enter an e-mail address.

3. Select **Replace or Swap a MAC address in an existing license file**.
4. Enter the License Authorization Code.
5. Enter switch or switch stack base MAC address(es). If replacing a license file that had multiple MAC addresses, reenter the MAC addresses including the new MAC address.
6. **(Optional)** Specify the License Bank name.

7. **(Optional)** Specify the License file name.

   You can rename a license file name before it is installed on a switch.

8. Click **Submit Request**.

   If you exceed the MAC replacement threshold, a message appears confirming that the MAC swap is unsuccessful. Select a different LAC entry and try again. If no other LAC entries appear in the list, contact technical support.

9. After the system displays“ `MAC swap successful`”, click **Return to License Bank Details**.

10. Select the transaction that contains the license file name with the new MAC address.

11. Click **Download**.

Special cases with software licensing

The following sections describe situations when software licensing can be lost or fail.

Downgrade of switch software followed by upgrade of switch software

On a stand-alone switch, if you downgrade from Release 5.4 or later software to Release 5.3 or earlier software, and then upgrade back to Release 5.4 or later software, the software license is lost.

In a stack, if you downgrade from Release 5.4 or later software to Release 5.3 or earlier software, and then upgrade back to Release 5.4 or later software, the license is retained. The system sets the operational license to Advanced Software and the installed license displays as None. Because Release 5.3 does not support software licensing, the license can be lost in the rare event that memory is reused. If this happens, you must reinstall the software license after the upgrade.

Base unit failure in a stack of two units

Avaya recommends that you not operate a stack of two switches with a software license based only on the base unit (BU) MAC address. If the base unit fails, after you reboot the former non-base unit (NBU), now a standalone switch, the switch is unlicensed.

To prevent the loss of the software license, Avaya recommends that you install a software license that contains the NBU MAC address.

Base unit failure in a stack of more than 2 units

Avaya recommends that you not install a license file when the system is operating in temporary base unit (TBU) mode.

In a stack, if you create a license file based on the MAC address of the base unit (BU), then designate another unit in the stack as the BU, then when you download the license file the system generates error messages and the license process fails.

Chapter 4: User interface fundamentals

This chapter provides basic information to help you understand the interfaces you can use to configure and manage an Avaya Ethernet Routing Switch. Available features depend on switch model and configuration.

ACLI concepts

Avaya Command Line Interface (ACLI) is a text-based interface that you can use for switch configuration and management. A common command line interface (CLI), ACLI follows the industry standard used for device management across Avaya products.

The command modes within ACLI are listed in order of increasing privileges and each mode is based on the user logon permission level. User logon permission is determined by a logon password as supplied by your system administrator.

You can access ACLI directly through a console connection, remotely through a dial-up modem connection, or in-band through a Telnet session.

You can use ACLI interactively or use the `configure network` command to load and execute ACLI scripts, manually loading the script in the console menu, or automatically loading the script at startup. For more information about the command, see Configuration file management procedures on page 54.

The following topics describe ACLI command modes, provide procedures to access ACLI, and describe ACLI help.

ACLI command modes

Avaya Command Line Interface (ACLI) provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- Router Configuration
- Application Configuration

- DHCP Guard Configuration
- RA Guard Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter ACLI in User EXEC mode and use the **`enable`** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Table 1: ACLI command modes

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC
`Switch>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`Switch#`
	`enable`	`exit`
		or
		`logout`

Global Configuration
`Switch(config)#`
	`configure terminal`	To return to Privileged EXEC mode, enter
		`end`
		or
		`exit`
		To exit ACLI completely, enter
		`logout`

Interface Configuration
`Switch(config-if)#`
You can configure the following interfaces:
• Ethernet
• VLAN
• Loopback
	From Global Configuration mode:
	To configure a port, enter `interface ethernet` *`<port number>`*.
	To configure a VLAN, enter `interface vlan` *`<vlan number>`*.
	To configure a loopback, enter `interface loopback` *`<loopback number>`*.
		To return to Global Configuration mode, enter
		`Exit`
		To return to Privileged EXEC mode, enter
		`end`
		To exit ACLI completely, enter
		`logout`

Router Configuration	From Global or Interface Configuration mode:	To return to Global Configuration mode, enter

Table continues…

Command mode and sample prompt	Entrance commands	Exit commands
`Switch(configrouter)#` You can configure the following routers: • RIP • OSPF • VRRP • ISIS	To configure RIP, enter `router rip`. To configure OSPF, enter `router ospf`. To configure VRRP, enter `router vrrp`. To configure IS-IS, enter `router isis`.	`exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.
Application Configuration `Switch(config-app)`	From Global, Interface or Router Configuration mode, enter `application`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.
DHCP Guard Configuration `Switch(config-dhcpguard)`	From Global, Interface, Router, Application Configuration mode, enter `ipv6 dhcp guard policy` *<policy_name>*.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.
RA Guard Configuration `Switch(config-raguard)#`	From Global, Interface, Router, Application Configuration mode, enter `ipv6 nd raguard policy` *<policy_name>*.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.

ACLI access procedures

Before you begin

- Connect to the switch with a console cable, connected directly to the console port, or use Telnet.
- To connect to the switch remotely, through Telnet, ensure that you enable remote access, and that the switch IP address is valid.
- Use a terminal, or computer with a terminal emulator, as the ACLI command station.
- If you use a console cable and console port, ensure that the terminal emulation program conforms to settings listed in the following table.

Property	Value
Baud Rate	9600 bps
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Terminal Protocol	VT100 and VT100/ANSI

Opening an ACLI session

Procedure

1. Connect to the switch.
2. Enter the password, if applicable.
3. At the ACLI Banner Screen, enter `CTRL+Y`.
4. To access ACLI, from the main menu, press `c` or scroll to `Command Line Interface`.
5. Press `Enter`.

ACLI help

This section describes help available in ACLI.

ACLI help is available at all levels.

ACLI list

From the Privileged EXEC mode, the ACLI list command **`show cli list`** displays a detailed view of the ACLI commands. Additionally, the verbose command, **`cli list verbose`** lists the CLI syntax for each command.

Command list

To obtain a list of all commands available from a prompt, enter a question mark (`?`).

Command options

To obtain a list of all options for a command, at the prompt enter a portion of a command followed by a space and a question mark (`?`).

Command names

To obtain a correct command name, at the prompt enter a portion of the command name, and then press the Tab key. The system displays the first unambiguous match for your selection. For example, when you enter `down + Tab`, the system displays `download`.

Command modes

To obtain a list of ACLI command modes available, enter `help modes`.

Commands organized by mode

To obtain a list of ACLI commands, organized by command mode, enter `help commands`. A short explanation of each command is included.

Keystroke shortcuts

To make using ACLI easier, use the keystroke shortcuts in the following table.

Key combination	Function
`Ctrl+A`	Start of line
`Ctrl+B`	Back 1 character
`Ctrl+C`	Abort command
`Ctrl+D`	Delete the character indicated by the cursor
`Ctrl+E`	End of line
`Ctrl+F`	Forward 1 character
`Ctrl+H`	Delete character left of cursor (Backspace key)
`Tab`	Command or parameter completion
`Ctrl+K` and `Ctrl+R`	Redisplay line
`Ctrl+N` or `Down arrow`	Next history command
`Ctrl+P` or `Up arrow`	Previous history command
`Ctrl+T`	Transpose characters
`Ctrl+U`	Delete entire line
`Ctrl+W`	Delete word to left of cursor
`Ctrl+X`	Delete all characters to left of cursor
`Ctrl+z`	Exit Global Configuration mode to Privileged EXEC mode
`?`	Context sensitive help
`Esc+C` and `Exc+U`	Capitalize character at cursor

Table continues…

Key combination	Function
`Esc+l`	Change character at cursor to lower case
`Esc+B`	Move back 1 word
`Esc+D`	Delete 1 word to the right
`Esc+F`	Move 1 word forward

ACLI pipe filter

Pipe (|) is used to display only a subset of information in the command output. To filter the command output, type the existing ACLI command followed by the pipe (|) symbol and then, the pipe filter command. The output contains only the lines specified in the pipe filter.

The following pipe filter functions are supported:

Filter function	Description
count	Counts the number of lines in the output of a command.
match	Displays only the output lines which match the given pattern.
except	Displays only the output lines which do not match the given pattern.
find	Displays the output of a command starting from the first line which matches the given pattern.
no-more	Temporarily disables pagination for the output of an ACLI command. When the lines of output exceed the terminal length, the entire output of the command is displayed and message does not appear to continue or quit.
head	Limits the output of a command to the first few lines. If limit is not specified, the first 10 lines appear.
tail	Limits the output of a command to the last few lines. If a number is not specified the last 10 lines are shown.

To see if a command supports the ACLI pipe filter functionality, enter the command followed by a question mark (?).

For more information about the functions, see ACLI pipe filter functions on page 57.

Count filter

This filter counts the number of lines in the output of a command.

Syntax

```
<ACLI command> | count
```

Example

```
#show running-config | count
```

```
Count: 100 lines
```

Display output matching a pattern

The match filter displays only the output lines that match the given pattern.

Syntax

`<ACLI command> | match <pattern> [field <number>] [ignore-case] [header <number>]`

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Examples

```
#show interfaces | match 1000 header 3
              Status                    Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
9          Enable  Up   Up   Enabled  Enabled     1000Mbps Full   Asymm
```

```
#show interfaces | match disabled field 5 ignore-case
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
11         Enable  Down Down Disabled Enabled
```

Ignore output that matches a pattern

The ignore filter displays only the output lines that do not match the given pattern. The lines matching the pattern are discarded.

Syntax

`<ACLI command> | except <pattern> [field <number>] [ignore-case] [header <number>]`

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.

Table continues…

Parameter	Description
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Example

```
#show interfaces | except down ignore-case header 3
              Status                    Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
9          Enable  Up   Up   Enabled  Enabled     1000Mbps Full   Asymm
```

Display output from the first match of a pattern

The find filter displays the output of a command starting from the first line that matches the given pattern.

Syntax

```
<ACLI command> | find <pattern> [field <number>] [ignore-case] [header
<number>]
```

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Example

```
#show interfaces | find 47 header 3
              Status                    Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
47         Enable  Down Down Enabled  Enabled
48         Enable  Down Down Enabled  Enabled
49         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
50         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
51         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
52         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
```

Do not paginate output of a single command

The no-more command filter temporarily disables pagination for the output of an ACLI command. When the lines of output exceed the terminal length, you are not prompted to continue or to quit but the entire output of the command continues to be displayed. The effect is similar to setting terminal length 0 but only for the current command.

Example

```
#show interfaces | no-more
```

Display only the first few lines of output

The head filter limits the output of a command to the first few lines. If a number is not specified then the first 10 lines are shown.

Syntax

```
<ACLI command> | head [<number>]
```

Parameter	Description
<number>	Specifies the number of lines to keep from the beginning of the output.

Example

```
#show interfaces | head
              Status                  Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
```

Display only the first few lines of output

The head filter limits the output of a command to the first few lines. If a number is not specified then the first 10 lines are shown.

Syntax

```
<ACLI command> | head [<number>]
```

Parameter	Description
<number>	Specifies the number of lines to keep from the beginning of the output.

Example

```
#show interfaces | head
              Status                     Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
```

Display only the last few lines of output

The tail filter limits the output of a command to the last few lines. If a number is not specified, then the last 10 lines are shown.

Syntax

```
<ACLI command> | tail {[<number>] | from-line <number> } [header
<number>]
```

Parameter	Description
<number>	Specifies the number of lines to keep from the end of the output.
from-line <number>	Specifies the line from which to start the output.
[header]	Same description as for the other commands which allow it.

Example

```
#show interfaces | tail 3
50         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
51         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
52         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
```

Regular expressions

Match, except, and find filters require a pattern parameter, which is a regular expression.

Pattern parameter	Description
regular expression	Zero or more branches separated by the pipe symbol '|' It matches anything that matches one of the branches.
branch	Zero or more pieces, concatenated. For instance, it matches a match for the first, followed by a match for the second.
piece	An atom possibly followed by `*', `+', or `?'. An atom followed by `*' matches a sequence of 0 or more matches of the atom. An atom followed by `+' matches a sequence of 1 or more matches of the atom. An atom followed by `?' matches a match of the atom, or the null string.

Table continues…

Pattern parameter	Description
atom	A regular expression in parentheses (matching a match for the regular expression), a range, `.' (matching any single character), `^' (matching the null string at the beginning of the input string), `$' (matching the null string at the end of the input string), a `\' followed by a single character (matching that character), or a single character with no other significance (matching that character).
range	A sequence of characters enclosed in `[ ]'. It normally matches any single character from the sequence. If the sequence begins with `^', it matches any single character not from the rest of the sequence. If two characters in the sequence are separated by `-', this is shorthand for the full list of ASCII characters between them (for example, `[0-9]' matches any decimal digit). To include a literal `]' in the sequence, make it the first character (following a possible `^'). To include a literal `-', make it the first or last character.
	If the pattern includes white spaces then it must be enclosed in quotation marks.
	To match characters which have a special meaning – one of *.+?^$()[]\ – they must be escaped. They must be preceded by a single backslash if the pattern is not in quotation marks and by double backslash if the pattern is enclosed in quotes.

Regular expression examples

Regular expression	Description
est	Matches a string containing “est”. For example, “testing”.
A(d+)r	Matches a string containing an ‘A’ followed by at least one ‘d’ followed by ‘r’. For example, “Address”.
^1	Matches a ‘1’ only at the beginning of a line.
192\.[0-9]+\.[0-9]+\.[0-9]+	Matches a string representing a valid IPv4 address starting with 192.
“192\\.[0-9]+\\.[0-9]+\\.[0-9]+”	Matches a string representing a valid IPv4 address starting with 192 when the pattern is enclosed in quotes. The un-escaped ‘.’ means “any single character” which would make the regular expression accept invalid addresses as well.

Enterprise Device Manager concepts

This section provides information to start and use Enterprise Device Manager (EDM) to monitor, manage, and configure the switches.

To manage the switch from a centralized location, using Configuration and Orchestration Manager (COM) 2.0 and higher, 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.

The following table compares EDM functions in the embedded version to the COM plug-in version.

Table 2: EDM functions: embedded version compared to COM plug-in version

EDM functions	Embedded version	Plug-in version
100% device configuration: device view, device-specific configuration	Yes	Yes
Stackable Device Web User Interface features	Yes	No
Centralized off-box multi-user element management: • user and device credential manager • user preference • SSO-based user access control • user-based Device Access Control (read only and read-write) • authentication through third party (RADIUS, Microsoft AD, Sun AM)	No	Yes
Centralized EM plug-in management (downloadable install and uninstall, upgrade, patch, and inventory view	No	Yes
User activity log and audit trail	No	Yes
Device performance monitoring and polling	Limited	High performance and low latency
Device-specific single-device wizards and template	No	Yes
Centralized syslog and trap viewer	No	Yes
Troubleshooting and diagnostic tools (ping, CLI*Manager, path-trace)	No	Yes

EDM is an embedded application that you can use for single-device element management and configuration through a standard web browser. Because EDM is embedded into Ethernet Routing Switch software, and the switch operates as a web server, you do not require additional client software.

Tested browsers

EDM has been tested with the following web browsers:

- Microsoft Internet Explorer versions 11.0
- Mozilla Firefox version 45.0.2

Memory requirements

If you install Configuration and Orchestration Manager on a computer to manage your switch, the computer must have at least 500 MB of free disk space.

There are no memory requirements to use EDM through a web browser.

Online help

Online help is context-sensitive and appears in a separate window in the web browser.

To obtain help for the current topic, click the help button on the toolbar in the work area.

If you are using EDM through a web browser, you need to download the help file to a TFTP server or a USB mass storage device and configure the EDM Help file path. For procedures, see Getting EDM online help files for embedded EDM on page 51.

Interface components

This section describes Enterprise Device Manager interface components.

The Enterprise Device Manager window includes the following parts:

- Navigation tree toolbar
- Switch Summary View
- Device Physical View
- EDM window
- Navigation tree
- Menu bar
- Toolbar
- Work area

Switch Summary View

The EDM initial view displays a Switch Summary View in the work area.

The Switch Summary tab displays basic switch information. This information-only display derives from the configuration tab **Edit** > **Chassis** > **Chassis**.

Following is a list of the fields on the **Switch Summary** tab:

- Hardware model
- Hardware version
- Firmware version

- Software version
- System up time
- System object identifier
- System contact
- System name
- System location

A Stack Information panel appears at the bottom of the Switch Summary View work area. It provides a description of your switch or the units in your switch stack.

This information includes the following:

- Unit number (for stacks) — also lists which unit is the base unit in a stack Switch type
- Description
- Running software version

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.

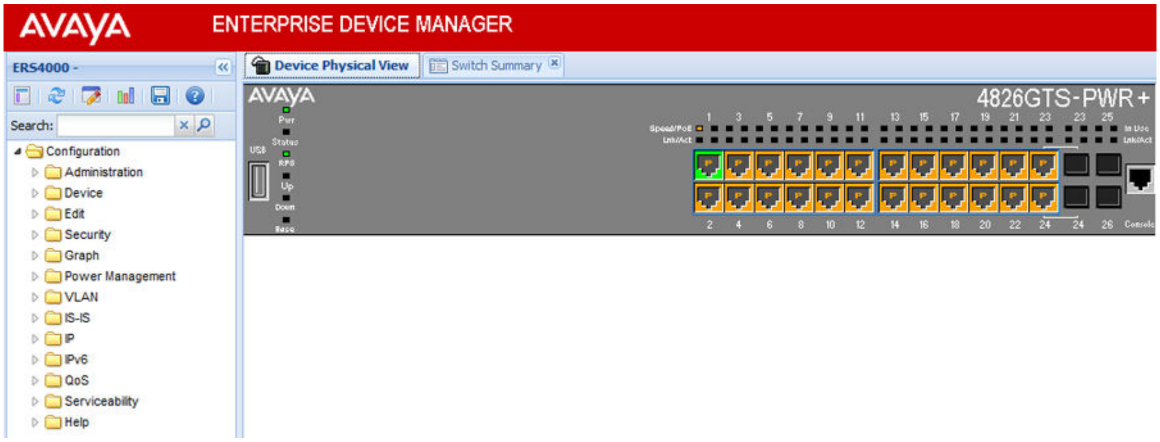
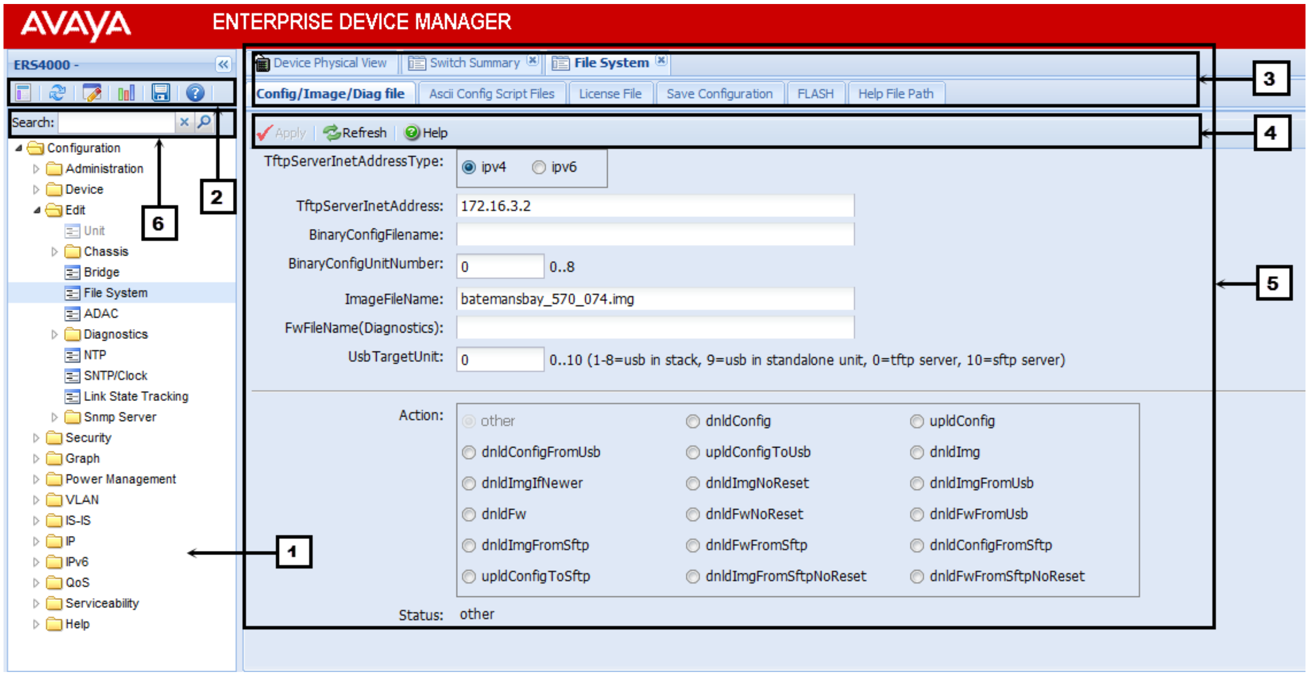


Figure 1: Device Physical View

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.



TftpServerInetAddressType: ● ipv4 ○ ipv6

TftpServerInetAddress: 172.16.3.2

BinaryConfigFilename:

BinaryConfigUnitNumber: 0 0..8

ImageFileName: batemansbay_570_074.img

FwFileName(Diagnostics):

UsbTargetUnit: 0 0..10 (1-8=usb in stack, 9=usb in standalone unit, 0=tftp server, 10=sftp server)

Action:

○ other ○ dnldConfig ○ upldConfig
○ dnldConfigFromUsb ○ upldConfigToUsb ○ dnldImg
○ dnldImgIfNewer ○ dnldImgNoReset ○ dnldImgFromUsb
○ dnldFw ○ dnldFwNoReset ○ dnldFwFromUsb
○ dnldImgFromSftp ○ dnldFwFromSftp ○ dnldConfigFromSftp
○ upldConfigToSftp ○ dnldImgFromSftpNoReset ○ dnldFwFromSftpNoReset

Status: other

Figure 2: EDM window

Navigation tree

The navigation tree displays available command topics as folders in a tree.

To open a folder or subfolder, click the arrow to the left of the folder or double-click the folder to display the available commands tabs.

To close a folder, click the arrow once.

To access a command tab, click the selection in the navigation tree.

Navigation tree toolbar

You can use the toolbar above the navigation tree to perform common functions more easily.

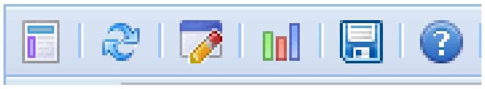


Figure 3: Toolbar

The following is a description of the toolbar button functions:

Button	Description
🗔	**Switch Summary**—You can use the **Switch Summary** toolbar button to open or reopen the Switch Summary tab.
🔄	**Refresh Status**—In addition to the existing refresh methods you can use the **Refresh Status** toolbar button to refresh the device status

Table continues…

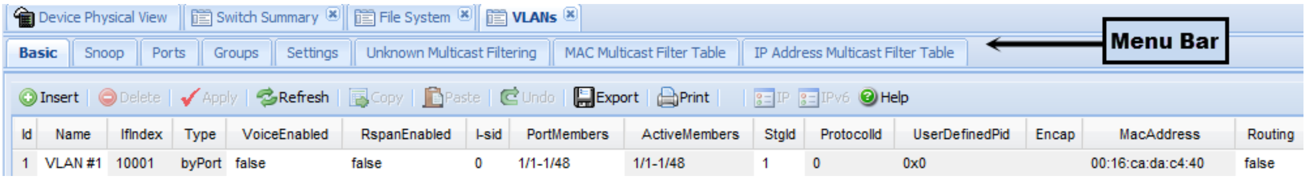
Button	Description
✎	**Edit Selected**—In addition to the existing edit methods, and depending on which object you select on the Device Physical View, you can use this toolbar button to open **Edit > Chassis**, **Edit > Unit**, or **Edit > Ports** tabs. If you do not select an object from the Device Physical View and you click the **Edit Selected** toolbar button, the **Edit > Chassis** tab opens.
📊	**Graph Selected**—Depending on which object you select on the Device Physical View, you can use this toolbar button to open **Graph > Chassis** or **Graph > Port** tabs. If you do not make a selection on the Device Physical View, or if you select Unit, the **Graph > Chassis** tab opens.
💾	**Save Config**—You can use the **Save Config** toolbar button to save the configuration to flash memory.
?	**Help Setup Guide**—This button connects you to the help setup guide for embedded EDM and it replaces the link that appeared on the top right of work panes.

Menu bar

The menu bar appears above the work area and consists of two rows of tabs.

The top row displays tabs that were accessed from the navigation tree during the active session. The tabs in this row, called primary tabs, are docked and available to reopen on demand. The docked tabs appear in the sequence that you accessed them.

When you click a primary tab from the menu bar, the associated secondary tabs appear in the second row and the default dialog box appears in the work area. Click any secondary tab to display its associated dialog box.



Id	Name	IfIndex	Type	VoiceEnabled	RspanEnabled	I-sid	PortMembers	ActiveMembers	StgId	ProtocolId	UserDefinedPid	Encap	MacAddress	Routing
1	VLAN #1	10001	byPort	false	false	0	1/1-1/48	1/1-1/48	1	0	0x0		00:16:ca:da:c4:40	false

Figure 4: Menu bar

If you want to open a dialog box without displacing the current open dialog box, you can go to the tab on the menu bar and undock the tab by using your mouse to drag and drop it into the work area. You can drag the dialog box to any location on the screen and you can toggle between the open dialog boxes to compare information and make changes. When you no longer need the undocked tab, you can use the three buttons on the upper right side of the tab to temporarily shrink it, re-dock it, or close it.

Important:

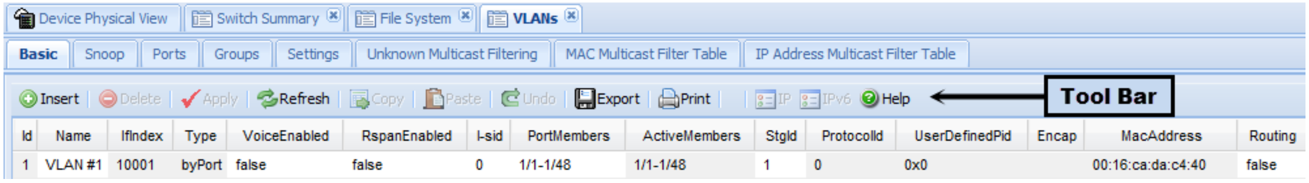
When you undock a tab to make changes, and then return to another open tab, in order to see the effects of the changes you must click the **Refresh** button on the tool bar.

In both rows of the menu bar, arrows can appear on the left and right sides when the number of open tabs exceeds the available space. You can use the arrows to scroll to a tab, or you can select the tab from the navigation tree.

To reduce the number of open tabs, click the **X** button on the top right of a tab to close it.

Tool bar

The tool bar, located below the menu bar, contains buttons that provide quick access to commonly used operational commands. Depending on the tab selected, different buttons can appear.



Id	Name	IfIndex	Type	VoiceEnabled	RspanEnabled	I-sid	PortMembers	ActiveMembers	StgId	ProtocolId	UserDefinedPid	Encap	MacAddress	Routing
1	VLAN #1	10001	byPort	false	false	0	1/1-1/48	1/1-1/48	1	0	0x0		00:16:ca:da:c4:40	false

Figure 5: Tool bar

The following table describes common tool bar buttons.

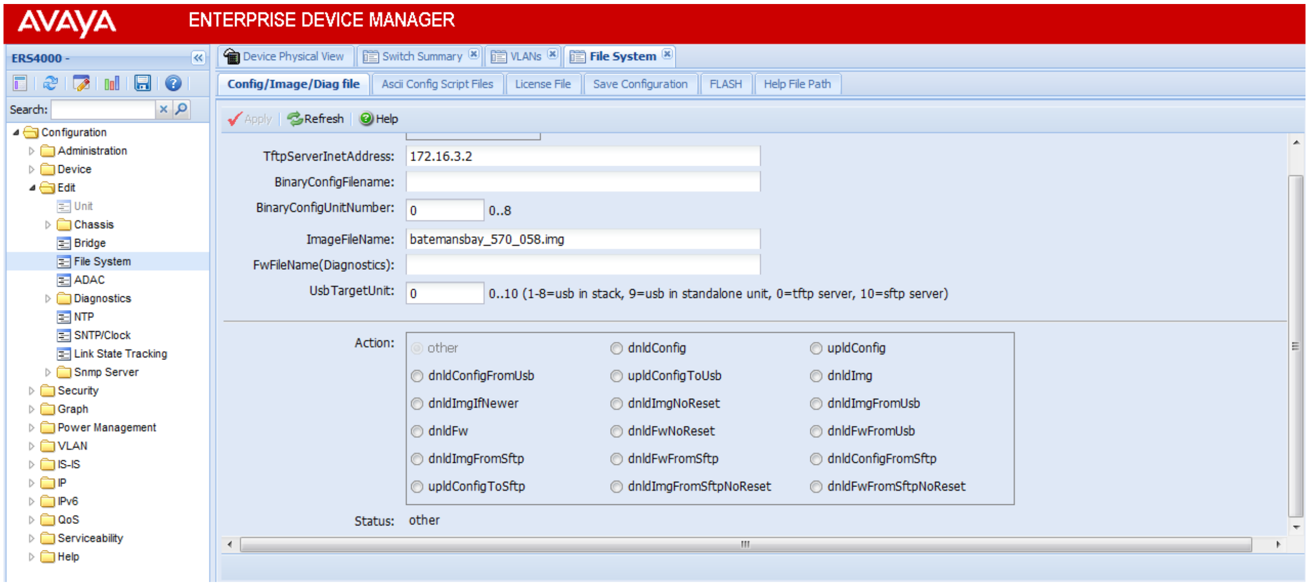
Table 3: Common tool bar buttons

Button	Name	Description
✓	Apply	Executes parameter changes.
⟳	Refresh	Refreshes screen data.
?	Help	Displays context-sensitive online help for the current dialog box.
⊕	Insert	Opens an insert dialog box. Submits the entry from the insert dialog box. The insert buttons appear only on panes where you can insert entries.
⊖	Delete	Removes a selected entry.

Work area

The work area, on the right side of the EDM page, displays the switch Device Physical View and dialog boxes related to the menu selections in the navigation tree. You can use the work area to view and configure switch parameters from the dialog boxes that appear in the work area.

See the following figure for an example of the work area for the **Edit** > **File System** > **Config/ Image/Diag file** dialog box.



TftpServerInetAddress: 172.16.3.2

BinaryConfigFilename:

BinaryConfigUnitNumber: 0 0..8

ImageFileName: batemansbay_570_058.img

FwFileName(Diagnostics):

UsbTargetUnit: 0 0..10 (1-8=usb in stack, 9=usb in standalone unit, 0=tftp server, 10=sftp server)

Action:

○ other	○ dnldConfig	○ upldConfig
○ dnldConfigFromUsb	○ upldConfigToUsb	○ dnldImg
○ dnldImgIfNewer	○ dnldImgNoReset	○ dnldImgFromUsb
○ dnldFw	○ dnldFwNoReset	○ dnldFwFromUsb
○ dnldImgFromSftp	○ dnldFwFromSftp	○ dnldConfigFromSftp
○ upldConfigToSftp	○ dnldImgFromSftpNoReset	○ dnldFwFromSftpNoReset

Status: other

Figure 6: EDM work area

Single-port configuration for EDM

You can apply configuration changes to single ports by using one of the following methods:

- From the Device Physical View, right-click a port, select **Edit** from the drop-down menu, and then click the appropriate tab.

  The following figure displays the drop-down menu for the selected port in the Device Physical View.

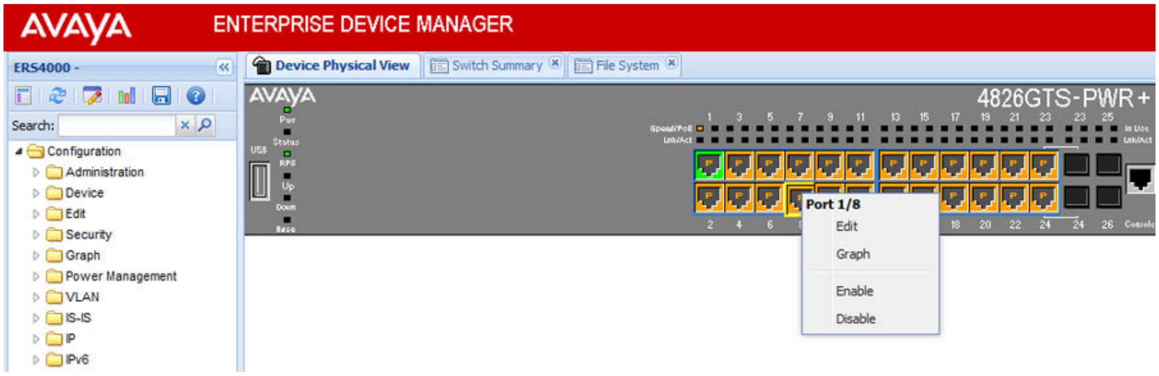
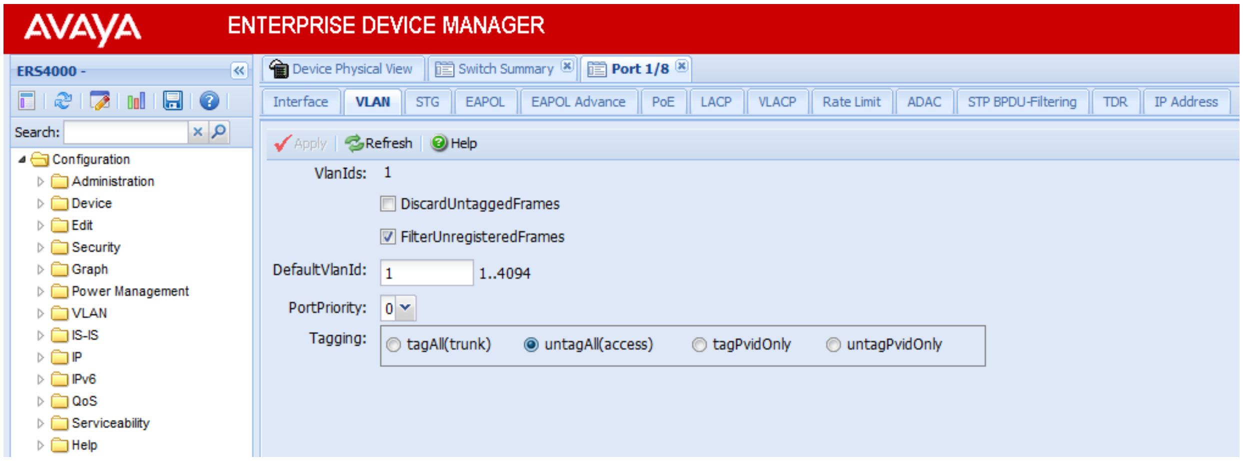


Figure 7: Device Physical View - port edit

The following figure displays the port edit work area with the **VLAN** tab selected.



VlanIds: 1

□ DiscardUntaggedFrames

☑ FilterUnregisteredFrames

DefaultVlanId: 1 1..4094

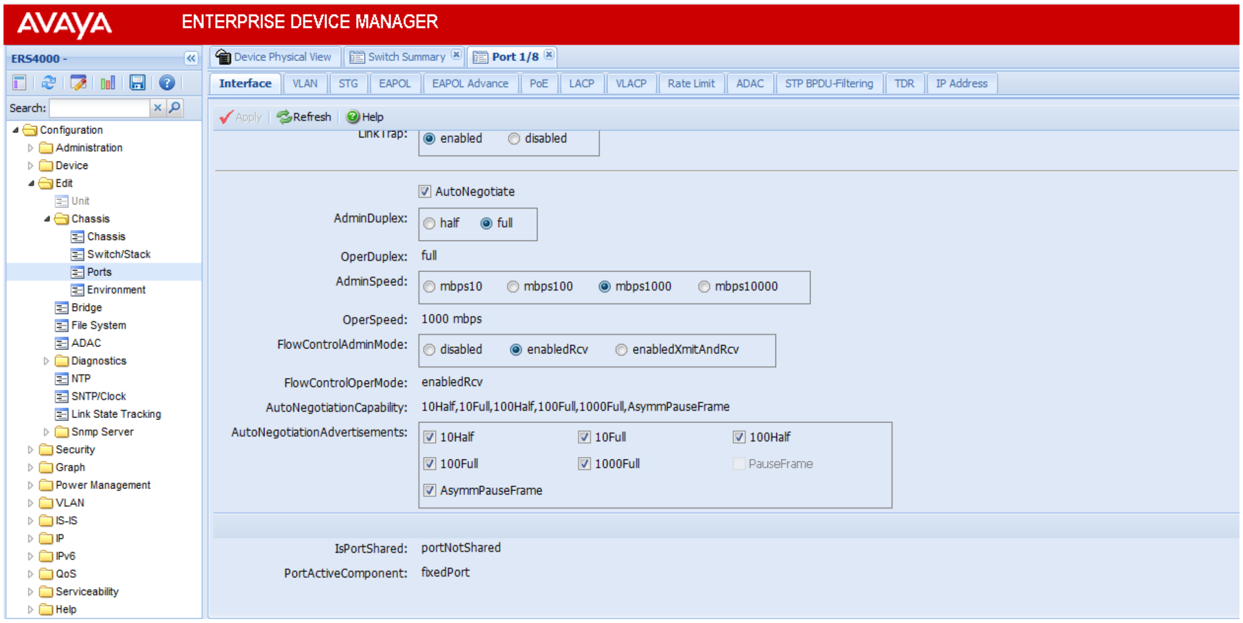
PortPriority: 0

Tagging: ○ tagAll(trunk) ● untagAll(access) ○ tagPvidOnly ○ untagPvidOnly

Figure 8: Port edit—VLAN tab

- From the Device Physical View, click a port, and then from the navigation tree select any tab from the **Edit** > **Chassis** > **Ports** work flow, and modify editable parameters.

  The following figure displays the **Edit** > **Chassis** > **Ports** work area with the **Interface** tab selected.



LinkTrap: ● enabled ○ disabled

☑ AutoNegotiate

AdminDuplex: ○ half ● full

OperDuplex: full

AdminSpeed: ○ mbps10 ○ mbps100 ● mbps1000 ○ mbps10000

OperSpeed: 1000 mbps

FlowControlAdminMode: ○ disabled ● enabledRcv ○ enabledXmitAndRcv

FlowControlOperMode: enabledRcv

AutoNegotiationCapability: 10Half,10Full,100Half,100Full,1000Full,AsymmPauseFrame

AutoNegotiationAdvertisements: ☑ 10Half ☑ 10Full ☑ 100Half ☑ 100Full ☑ 1000Full □ PauseFrame ☑ AsymmPauseFrame

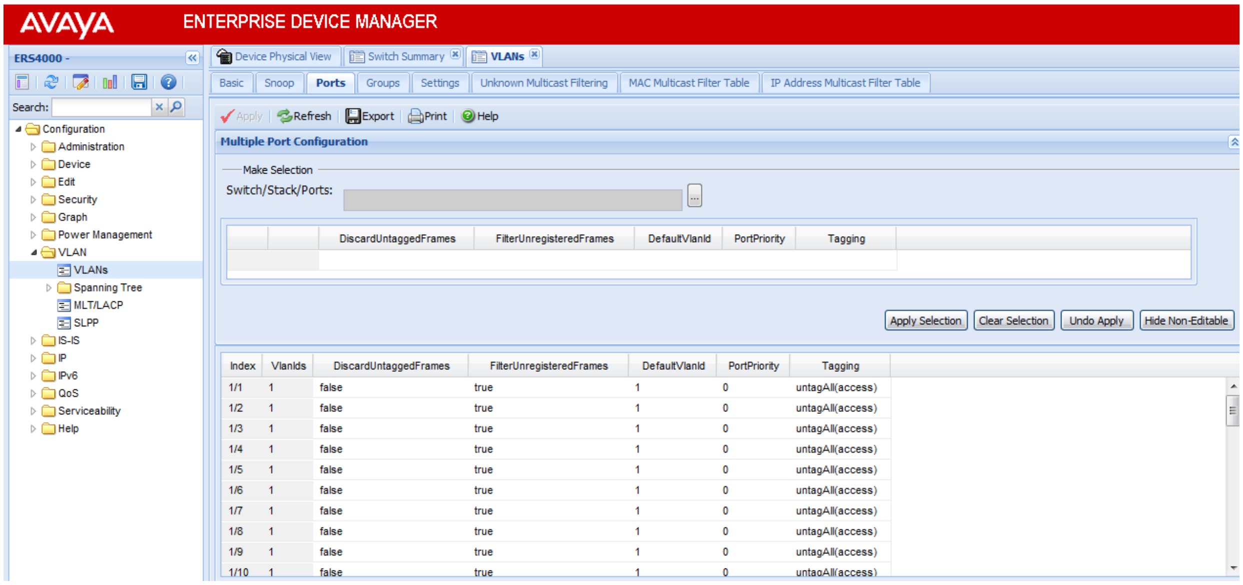
IsPortShared: portNotShared

PortActiveComponent: fixedPort

Figure 9: Edit > Chassis > Ports—Interface tab

- From the navigation tree, select a port-related tab from a specific, applicable feature work area (for example, VLAN, VLANs, Ports), and double-click a cell under an editable parameter column heading in the appropriate port row of the table.

  The following figure displays the **VLAN** > **VLANs** > **Ports** tab work area.



Index	VlanIds	DiscardUntaggedFrames	FilterUnregisteredFrames	DefaultVlanId	PortPriority	Tagging
1/1	1	false	true	1	0	untagAll(access)
1/2	1	false	true	1	0	untagAll(access)
1/3	1	false	true	1	0	untagAll(access)
1/4	1	false	true	1	0	untagAll(access)
1/5	1	false	true	1	0	untagAll(access)
1/6	1	false	true	1	0	untagAll(access)
1/7	1	false	true	1	0	untagAll(access)
1/8	1	false	true	1	0	untagAll(access)
1/9	1	false	true	1	0	untagAll(access)
1/10	1	false	true	1	0	untagAll(access)

Figure 10: VLAN > VLANs—Ports tab

Multiple Port Configuration for EDM

When you need to apply the same configuration changes to more than one port, you can use the Multiple Port Configuration function in any the following ways:

- In the **Device Physical View**, hold down the **Ctrl** key and click the ports. Then select the appropriate tab in the **Edit** > **Chassis** > **Ports** work area to configure the ports.
- In the **Device Physical View**, hold down the **Ctrl** key and click the ports you want to configure. Then right-click and select **Edit** from the menu.
- In the **Device Physical View** click and drag to surround a group of related ports. Then select the appropriate tab in the **Edit** > **Chassis** > **Ports** work area to configure the ports.
- In the **Device Physical View**, click and drag to surround a group of related ports. Then right-click and select **Edit** from the menu.

The system can generate error messages if you apply a change to all ports when some ports in the list do not support the change. The error messages provide only the error information and do not list individual ports.

The following sections use the **Edit** > **Chassis** > **Ports** > **Interface** tab work area to describe the available Multiple Port Configuration functions.

In the work area for any of the **Edit** > **Chassis** > **Ports** tabs, the following two panes appear in the default view:

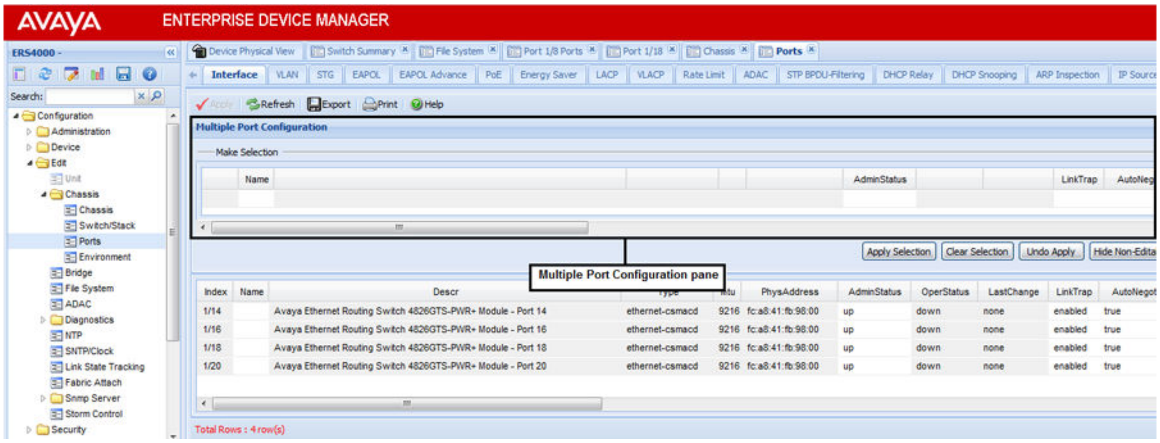
- Multiple Port Configuration pane—Provides port selection for one port, several ports, or all ports, and configurable port parameters
- Tab work pane—Displays existing configuration information for the feature and configurable cells for individual ports

With Multiple Port Configuration you can perform the following:

- Hide non-editable fields from the multiple configuration pane so that you choose to view only those fields that can be configured.
- Select an individual port or a group of ports from the Port Editor.
- Select all ports from the Port Editor, if you are on a feature tab. If you used **Edit** > **Chassis** > **Ports** you already selected the ports on the Device Physical View.
- Double-click any or all of the editable fields to change the configuration parameter.
- Clear your selections.
- Apply your selections.
- Undo the application of your selections.

You can expand or collapse the Multiple Port Configuration pane by clicking the Multiple Port Configuration task bar. The Multiple Port Configuration pane is expanded by default.

The following figure displays the tabs available in the **Edit** > **Chassis** > **Ports** work flow, with the **Interface** tab selected and the **Multiple Port Configuration** pane expanded.



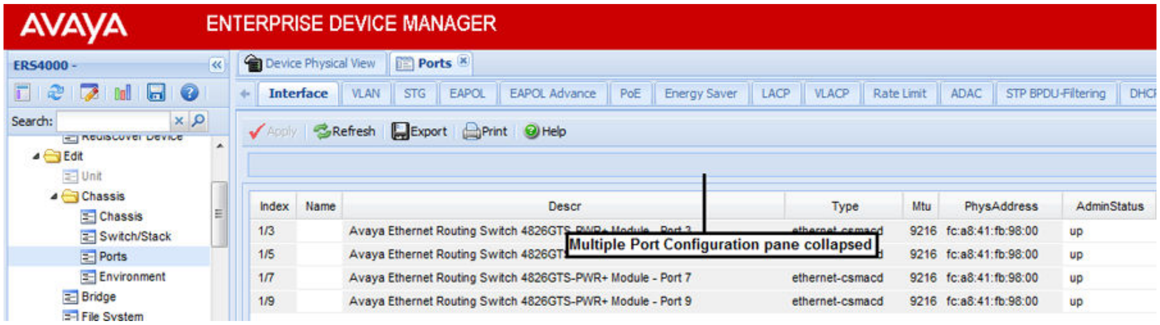
Multiple Port Configuration pane

Index	Name	Descr	Type	Mtu	PhysAddress	AdminStatus	OperStatus	LastChange	LinkTrap	AutoNegot
1/14		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 14	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/16		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 16	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/18		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 18	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/20		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 20	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true

Total Rows : 4 row(s)

Figure 11: Interface tab—Multiple Port Configuration pane expanded

The following figure displays the **Edit** > **Chassis** > **Ports** > **Interface** tab with the **Multiple Port Configuration** pane collapsed.



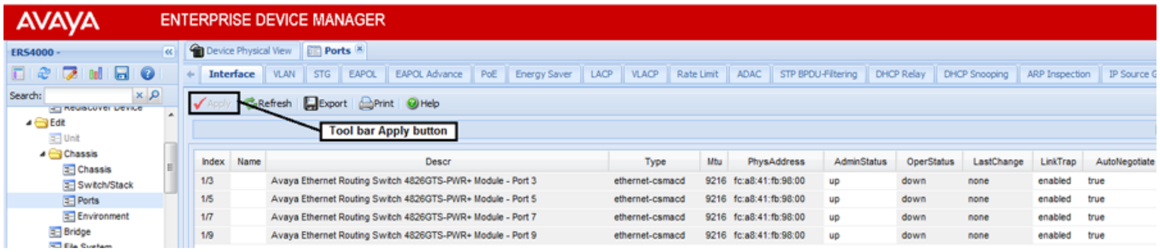
Multiple Port Configuration pane collapsed

Index	Name	Descr	Type	Mtu	PhysAddress	AdminStatus
1/3		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 3	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up
1/5		Avaya Ethernet Routing Switch 4826GT	d	9216	fc:a8:41:fb:98:00	up
1/7		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 7	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up
1/9		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 9	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up

Figure 12: Interface tab—Multiple Port Configuration pane collapsed

Changes you make to a port configuration using Multiple Port Configuration are applied to the switch configuration only after you click **Apply** on the work area toolbar.

The following figure displays the location of the **Apply** button on the work area toolbar.



Index	Name	Descr	Type	Mtu	PhysAddress	AdminStatus	OperStatus	LastChange	LinkTrap	AutoNegotiate
1/3		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 3	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/5		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 5	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/7		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 7	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true
1/9		Avaya Ethernet Routing Switch 4826GTS-PWR+ Module - Port 9	ethernet-csmacd	9216	fc:a8:41:fb:98:00	up	down	none	enabled	true

Figure 13: Toolbar Apply button

Enterprise Device Manager procedures

About this task

This section contains procedures for starting and using Enterprise Device Manager (EDM) on your switch. You can use EDM software on the switch; you do not need to install a client-based application on your computer.

Configuring EDM through ACLI

This section describes how to enable and configure the Enterprise Device Manager (EDM) using ACLI.

Enabling the web server using ACLI

About this task

The web server is enabled by default. If you assigned an IP address to the switch, you can access EDM.

If you have disabled the web server, you can use the following procedure to enable and manage the web server using ACLI. After you enable the web server, you can start EDM.

For more information about the web server, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable the web server, enter the following command:

```
web-server enable
```

Disabling the web server using ACLI

About this task

Use the following procedure to disable the web server using ACLI. After you disable the web server, you cannot start EDM.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To disable the web server, enter the following command:

   ```
   no web-server enable
   ```

Displaying the web server status using ACLI

About this task

Use the following procedure to display the web server status using ACLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To display the web server status, enter the following command:

   ```
   show web-server
   ```

Variable definitions

The following table describes the parameters for the `show web-server` command.

Variable	Definition
disable	Disable HTTP access.
enable	Enable HTTP access.
show	Show web server status.

Starting EDM

To configure and maintain your switch through a web-based graphical user interface, use the following procedure to start EDM.

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.
- Note the password.
- Open one of the supported web browsers.

About this task

Follow this procedure to open an EDM session on your switch.

Procedure

1. In a supported web browser, enter the IP address of the switch using one of the following formats:
   - `http://<IP Address>`
   - `https://<IP Address>`
2. Enter the user name.
3. Enter the password.
4. Click **Log On**.

Using shortcut menus

About this task

In the EDM Device Physical View, you can use shortcut menus to edit objects and apply changes.

Procedure

1. In the **Device Physical View**, select an object.
2. Right-click the object.
3. Select a function from the list.

Variable definitions

Use the data in the following table to use the Device Physical View.

Variable	Definition
Unit	
Edit	Displays the Edit unit dialog box and tabs.
Refresh Status	Refreshes switch status.

Table continues…

Variable	Definition
Refresh PoE Status	Refreshes the PoE status only to units equipped with Power over Ethernet.
Refresh Port Tooltips	Refreshes the port tooltip data. Port tooltip data contains the Slot/Port, PortName, and PortOperSpeed.
Identify Unit	Identifies the switch units.
Port	
Edit	Displays the Edit port dialog box and tabs.
Graph	Displays the graph port dialog box and tabs.
Enable	Enables the port administratively.
Disable	Shuts down the port administratively.

Opening folders and tabs

The following section describes how to navigate around Enterprise Device Manager (EDM) and open folders and tabs.

Navigating EDM

About this task

Use the following procedure to navigate EDM.

Procedure

1. In the navigation pane, click the arrow located to the left of a folder to display the subfolders in the tree.
2. If there is a subfolder, double-click the folder or click the arrow to open the subfolder.
3. The primary tabs appear under the folders and subfolders. Click a tab to open it in the work area.

Undocking tabs

About this task

To improve certain types of configuration, you can view more than one tab at a time. To view more than one tab, you use the undock function to activate a previously-opened tab from the menu bar.

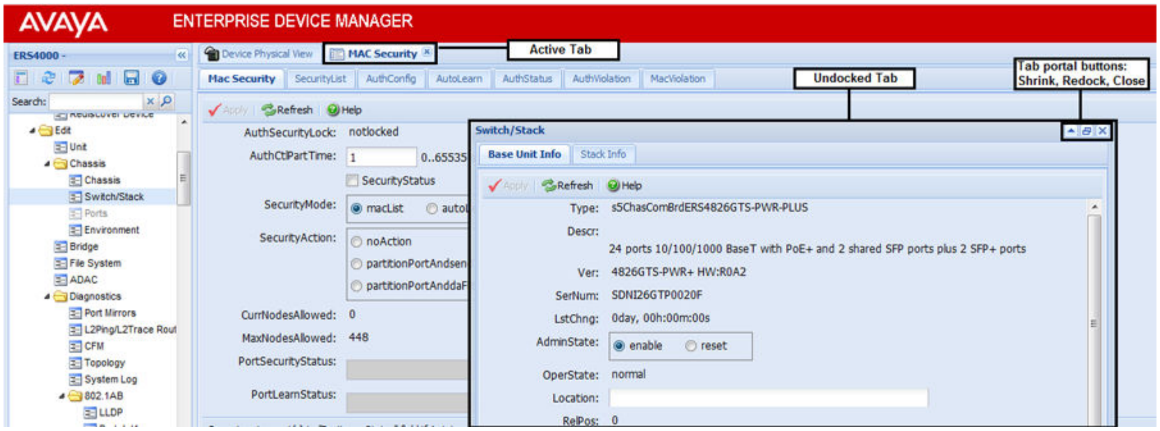
Important:

When you undock a tab to make changes, then return to another open tab, in order to see the effects of the changes you must click the **Refresh** button on the tool bar.

Procedure

1. From the menu bar, drag and drop the tab you want to open.

2. To reposition the tab in the work area, click and drag the title bar of the tab.



AuthSecurityLock: notlocked

AuthCtlPartTime: 1 0..65535

□ SecurityStatus

SecurityMode: ● macList ○ autol

SecurityAction: ○ noAction ○ partitionPortAndsen ○ partitionPortAnddaF

CurrNodesAllowed: 0

MaxNodesAllowed: 448

PortSecurityStatus:

PortLearnStatus:

Type: s5ChasComBrdERS4826GTS-PWR-PLUS

Descr: 24 ports 10/100/1000 BaseT with PoE+ and 2 shared SFP ports plus 2 SFP+ ports

Ver: 4826GTS-PWR+ HW:R0A2

SerNum: SDNI26GTP0020F

LstChng: 0day, 00h:00m:00s

AdminState: ● enable ○ reset

OperState: normal

Location:

RelPos: 0

Figure 14: Undocking and docking tabs

Docking tabs

About this task

You can re-dock an undocked tab using either of the following methods.

Procedure

To re-dock a tab, do one of the following:

- On the undocked tab, click the dock-back button (the middle button on the top right of the panel).
- On the undocked tab, click the collapse button (left button on the top right of the panel) to temporarily minimize the panel.

Using dialog boxes

Many EDM dialog boxes contain editable fields where you can enter parameter values.

Some of those parameters have predetermined values. For example, you can enable or disable a port.

Other parameter values are ranges of values or user-determined values. For example, the value for the Location on the **Base Unit Info** tab is a location name you can choose and enter.

Editable fields in EDM dialog boxes appear in white.

EDM dialog box buttons

The following table describes buttons that appear in the EDM dialog boxes and tabs. Not all buttons appear in all dialog boxes.

Table 4: EDM dialog box buttons

Button	Description
Apply	Apply the changes you entered in fields on a tab or dialog box. The button is unavailable until you change a parameter.
Insert	Open a dialog box to create a new entry for a table; then, from the dialog box, insert the new entry in the table.
Delete	Delete a selected entry.
Refresh	Refresh the information in the window. Every time you click **Refresh**, the switch polls the system and displays new information.
Close	Close the tab or dialog box and discard changes you made to fields.
Help	Open context-sensitive Online Help.
Stop	Stop the current action.
Copy	Copy selected items to your computer memory clipboard.
Paste	Paste the contents of your computer clipboard.
Undo	Undo last action.
Export	Copy data to external media.
Print	Print the contents of any displayed table.
Graph	Graph selected data.
Export (on Graph dialog boxes)	Save the current table in ASCII format in a file you specify. The table contains tabs that you can use to import this file into a text editor or spreadsheet for further analysis.
Clear Counters	Clear the existing number of counters and restart the counters.
Clear all	Clear the numbers of all statistics and restart the count.

Editing a dialog box

About this task

Use the following procedure to edit a dialog box.

Procedure

1. In the work area, double-click the field you want to edit.
2. Select a value from the list of predetermined values or enter the value for a field without preset values.

   Important:

   Enter an IP address in decimal format: <xxx>.<xxx>.<xxx>.<xxx>.

   Enter a MAC address in hexadecimal format: xx:xx:xx:xx:xx:xx.

   Time is a value based on the delta from the switch boot-up time.
3. Click **Apply**.

Inserting an entry in a dialog box

About this task

Use the following procedure to insert an entry in a dialog box.

Procedure

1. On the tool bar, click **Insert** .
2. Enter changes in the Insert dialog box.
3. Click **Insert** to submit the entry and return to the active tab in the work area.
4. On the toolbar, click **Apply** to commit the change to the configuration. The system refreshes the view and errors display in a browser pop-up window.

Deleting an entry from a dialog box

About this task

Use the following procedure to delete an entry from a dialog box.

Procedure

1. Highlight the entry.
2. Click **Delete**.

Editing objects

You can edit objects in the Device Physical View from the navigation tree or the shortcut menu. Changes are not applied to the running configuration until you click **Apply**.

Editing an object using the shortcut menu

About this task

Use the following procedure to edit an object using the shortcut menu.

Procedure

1. On the Device Physical View, you can:
   - Right-click an object.
   - Press **Ctrl+click** to select several objects; then right-click.
   - Click and drag to select a group of objects; then right-click.
   - Click an entire device; then right-click.
2. From the list, click **Edit**.
3. Edit the applicable tab in the work area.
4. Click **Apply**.

Editing file system elements

About this task

Use the procedure and job aid in this section to edit file system elements.

Procedure

1. Click the **Edit** arrow to open the Edit menu.
2. Click **File System** to open the File System tab in the work area.

   For more information about configuration files and licensing, see “Configuration files fundamentals” and “Feature licensing fundamentals” in *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102.

Job aid—File System

The following table describes the tabs in the File System work area.

Tab	Description
Config/Image/Diag file	Use this tab to view information about and acquire image, configuration, and firmware files.
Ascii Config File	Use this tab to acquire ASCII configuration files.
License File	Use this tab to view and manage software licensing.
Save Configuration	Use this tab to save the current configuration manually or automatically.
FLASH	Use this tab to view the current number of erase or writes on a unit or stack.
Help File Path	Use this tab to designate the file path to the EDM help files. You can use a USB mass storage device or a TFTP server.

Job aid—navigation tree

The following table describes the folders and subfolders in the navigation tree.

Folder	Description
Administration	Use the tabs associated with the sub-folders in the Administration folder to perform the following functions: • Quick Start—Set up IP/Community/VLAN and Trap Receiver. • Remote Access—Enable or disable telnet, SNMP, web page, and SSH. • Run Script—Configures parameters for the switch, according to Avaya best practices. Run Scripts are available for IP Office, LLDP, and ADAC.

Table continues…

Folder	Description
	• MIB Web Page—Perform MIB Walk.
Device	Rediscover Device—Use the Rediscover Device selection to refresh the session. ⚠ **Warning:** All existing tabs are lost.
Edit	Use the tabs associated with the subfolders in the Edit folder to view or change parameters for the currently-selected object. Subfolders in the Edit folder are: • Unit • Chassis: Chassis, Switch/Stack, Ports, and Environment • Bridge • File System • ADAC • Diagnostics: Port Mirrors, L2Ping/L2 Trace Route, CFM, Topology, System Log. 802.1AB: LLDP, Port dot1, Port dot3, Port MED, Avaya • NTP • SNTP/Clock • Link State Tracking • Fabric Attach • Snmp Server: MIB View, User, Community, Host, Notification Control • Storm Control
Security	Use the tabs associated with the sub-folders in the Security folder to view or change security settings. Sub-folders in the Security folder are: • General • MAC Security • DHCP Snooping • Dynamic ARP Inspection (DAI) • IP Source Guard (IPSG) • 802.1X/EAP • Web/Telnet/Console • SSH/SSL

Table continues…

Folder	Description
	• RADIUS • TACACS+
Graph	Use the tabs associated with the subfolders in the Graph folder to view statistics and produce graphs of the statistics. Subfolders in the Graph folder are: • Chassis • Port—To view or graph statistics for a port, first select a port on the Device Physical View.
Power Management	Use the tabs associated with the subfolders in the Power Management folder to view and configure Power over Ethernet (PoE) settings and to view and configure Energy Saver settings. Subfolders in the Power Management folder are: • PoE • Energy Saver PoE is only available for switches equipped with Power over Ethernet.
VLAN	Use the tabs associated with the subfolders in the VLAN folder to configure or view information about VLANs, Spanning Tree, and Multi-Link Trunking. Subfolders in the VLANs folder are: • VLANs • Spanning Tree: Globals, STG, RSTP, MSTP • MLT/LACP • SLPP
IS-IS	Use the tabs associated with the subfolders in the IS-IS folder to configure or view information about SPBM. Sub-folders in the IS-IS folder are: • IS-IS • SPBM • Stats
IP	Use the tabs associated with the subfolders in the IP folder to configure IP routing functions. Subfolders in the IP folder are: • IP

Table continues…

Folder	Description
	• TCP/UDP • OSPF • RIP • VRRP • IGMP • PIM • DHCP Relay • UDP Forwarding • Policy
IPv6	Use the tabs associated with the subfolders in the IPv6 folder to set up IPv6 routing functions. Subfolders in the IPv6 folder are: • IPv6 • FHS • MLD • TCP/UDP
QoS	Use the tabs associated with the subfolders in the QoS folder to configure quality of service and set up QoS policies and filters. Subfolders in the QoS folder are: • QoS Devices • QoS Rules • QoS • QoS Agent • QoS UBP/Traffic Profile • QoS Queue Stats
Serviceability	Use the tabs associated with the subfolders in the Serviceability folder to monitor traffic flows using IPFIX, and to monitor and configure remote monitoring. Subfolders in the Serviceability folder are: • IPFIX • RMON: Alarms, Control • SLA monitor

Table continues…

Folder	Description
Help	Use the tabs associated with the subfolders in the Help folder to access help and support for the following: • Device Manager Basic • Support Portal (Avaya) • Legend: Up, Down, No Link, Standby, Testing, Unmanageable, and Loopback.

Example 1: Configuring multiple Interface ports using EDM

About this task

The following procedure provides sample steps for configuring multiple interface ports using the Multiple Port Configuration function and the **Edit** > **Chassis** > **Ports** > **Interface** work flow. When you use this work flow you must first select ports on the Device Physical View.

Procedure

1. On the Device Physical View, select a port or ports.
2. From the navigation tree, double-click **Edit**.
3. From the Edit tree, double-click **Chassis**.
4. From the Chassis tree, click **Ports**.
5. Click the **Interface** tab.
6. To change the configuration of the selected ports, in the Multiple Port Configuration pane, double-click the cell beneath the column heading that represents the parameter you want to change and do one of the following:
   - Select a value from a drop-down list.
   - Type a value in the cell.
7. In the **Make Selection** pane, click **Apply Selection**.

   The changes appear in the table.
8. On the **Interface** tab toolbar, click **Apply** to apply the changes to the switch configuration.

Example 2: Configuring multiple ports using EDM

The following procedure provides sample steps for configuring multiple ports using the Multiple Port Configuration function and the **Security** > **MAC Security** > **AutoLearn** workflow. When you use this, and similar workflows, you can select ports directly from the Multiple Port Configuration pane on the configuration tab. If you use the **Edit** > **Chassis** > **Ports** workflows you must first select ports on the Device Physical View.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. From the Security tree, click **MAC Security**.
3. Click the **AutoLearn** tab.

4. In the work area, in the **Make Selection** section of the **Multiple Port Configuration** pane, click the **Switch/Stack/Ports** ellipsis (...) to open the **Port Editor** dialog.
5. In the **Port Editor** window, click the ports you want to configure.

   Note:

   To configure all ports, click **All**.
6. Click **OK** to return to the Make Selection pane.

   The ports you selected appear in the **Switch/Stack/Ports** section.
7. To change the configuration of the selected ports, in the **Multiple Port Configuration** pane, double-click the cell beneath the column heading that represents the parameter you want to change and perform one of the following actions:
   - Select a value from a drop-down list.
   - Type a value in the cell.
8. In the **Make Selection** pane, click **Apply Selection**.

   The changes appear in the table.
9. On the **AutoLearn** tab toolbar, click **Apply** to apply the changes to the configuration.

Job aid—Buttons and dialog boxes in the Multiple Port Configuration pane

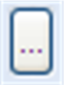
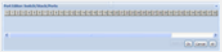
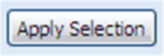
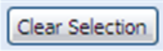
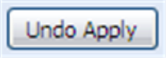
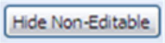
Button or dialog box name	Button or dialog box	Description
Switch/Stack/Ports:		Opens the Port Editor dialog box.
Port Editor		Provides a list of all ports on the switch or stack. • Click **OK** to accept port selections and return to the Multiple Port Configuration pane. • Click **Cancel** to return to the Multiple Port Configuration pane. • Click **All** to select all ports and return to the Multiple Port Configuration pane.
Apply Selection		Applies port selections and parameter changes to the Multiple Port Configuration pane and the port data table for review.
Clear Selection		Clears Multiple Port Configuration selections.

Table continues…

Button or dialog box name	Button or dialog box	Description
Undo Apply		Deletes port changes applied in the Multiple Port Configuration pane.
Hide Non-Editable		Displays only those parameters that are editable in the Multiple Port Configuration pane for the selected ports.

Graphing statistics

About this task

You can graph statistics for an entire device, a group of ports, or a single port.

Procedure

1. In the Device Physical View, select one of the following:
   - A port
   - A group of ports
   - A device
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, select one of the following:
   - **Chassis**
   - **Port**
4. In the work area, select a tab.
5. On the tab, select information to graph. To export the information to another application, on the task bar click **Export Data**.
6. To create the graph, on the task bar, click a graph type.

Getting EDM online help files for embedded EDM

Because help files are not included with the embedded EDM software files on the switch, you need to download the help files to a TFTP destination and use ACLI to configure a path from your switch to the help files. You can also use a USB mass storage device to contain help files for switches equipped with a USB port.

If you are using COM to manage your switch, help resides with COM and you do not need to use these procedures.

Downloading help files

Before you begin

- An available TFTP server— ensure that the TFTP path differs from the path you use to download switch software,

  OR

  A USB mass storage device and switch equipped with a USB port

About this task

Use the following procedure to download help files.

⚠ **Caution:**

Do not install EDM help files on a PCMCIA or Flash card.

Procedure

1. To obtain EDM help files for the embedded element manager, perform one of the following actions:
   - Go to the Avaya support site at http://support.avaya.com and locate the help files for the appropriate product.

     OR
   - Select the help file from the software CD-ROM.
2. Perform one of the following actions:
   - Download the help file to a TFTP server.

     OR
   - Download the help file to a USB mass storage device.
3. Unzip the help file in the TFTP server directory.

Configuring the path to the help files using ACLI

About this task

Use the following procedure to configure the path to the help files.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```
2. At the command prompt, enter the following ACLI command:

   ```
   edm help-file-path <path name> <tftp address | usb> <filename>
   ```

Variable definitions

The following table describes the parameters for the `edm help-file-path` command.

Variable	Definition
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.
TFTP address	Specifies the EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently. ⚠ **Warning:** Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.
usb <*unit*>	Specifies the unit number where the USB mass storage device that contains the help files resides. The unit number is an integer from 1 through 8.

Configuring the help file path using EDM

About this task

Use the following procedure to configure the path to the help files.

Procedure

1. In the navigation tree, double-click **Edit** or click the Edit arrow to open the Edit menu.
2. Click **File System** to open the File System work area.
3. In the work area, click the **Help File Path** tab.
4. In the Help TFTP Source Directory Path field, enter the path to the help file storage location; for example, tftp://aaa.bbb.ccc.ddd/file_name, usb://file_name, or usb://unit number/file_name.

Displaying USB file information using EDM

About this task

Displays the general information of the files on a USB flash device.

Procedure

1. From the navigation tree, click **Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

Chapter 5: Configuration files fundamentals

This chapter provides fundamental information about working with configuration files.

Configuration files are ASCII text files that allow the administrator to change the switch configuration quickly.

Procedures to manage binary configuration files are included in the Enterprise Device Manager section.

Procedures for Universal Serial Bus (USB) devices apply only to switch models with USB ports.

ACLI configuration files

You can use ACLI to display, store, and retrieve configuration files, and to save the current configuration.

Configuration file management procedures

About this task

Perform the procedures in this section to display, store, restore, and save configuration files using ACLI. For a list of the command variables and definitions, see Variable definitions — ACLI commands on page 56.

Viewing current configuration using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `show running-config`.

Saving current configuration to SFTP server using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy running-config sftp [verbose] [module <applicationModules>] [filename <WORD>] ([address {<A.B.C.D> | <ipv6addr>}]) username <WORD> [password]`.

Saving current configuration to TFTP server using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy running-config tftp [address {<A.B.C.D> | <WORD>}] [module <applicationModules>][filename <WORD>][verbose]`

Saving current configuration to USB device using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy running-config usb [filename <WORD>][module <applicationModules>][unit<1-8>] [verbose]`

Saving current configuration to flash memory using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy config nvram`.

Restoring system configuration from USB device using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy config usb {filename <name> | unit <1-8>}`.

Restoring system configuration from TFTP using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy tftp config address <A.B.C.D> | <WORD> filename <name>`.

Restoring system configuration from SFTP using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy sftp config address <A.B.C.D> | <WORD> filename <name> username <WORD>[password]`.

Copying stack unit configuration to standalone switch using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter `copy [ tftp | sftp ] config address <A.B.D.C> | <WORD> filename <name> unit <unit number>`.

Downloading a configuration file automatically using ACLI

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter `configure network load-on-boot {disable | use-bootp |use-config} address <A.B.C.D> | <ipv6_address> filename <name>` to configure a switch or stack to automatically load a configuration file.

Variable definitions — ACLI commands

The following table describes the **`copy running-config`** command variables.

Variable	Definition
{tftp | sftp | usb}	Specifies whether to save the file to a TFTP or SFTP server or a USB mass storage device. **Note:** Not all switch models have a USB port.
address *<A.B.C.D>* | *<WORD>*	Specifies the address of the TFTP or SFTP server. • A.B.C.D—specifies the IP address • WORD—specifies the IPv6 address
filename *<name>*	Specifies the configuration file name.
username *<WORD>*	Specifies the username for downloading a configuration file automatically using ACLI.
[password]	Specifies the password for downloading a configuration file automatically using ACLI.

The following table describes the **copy config tftp unit** command variables.

Variable	Definition
address <*A.B.C.D*> | <*WORD*>	Specifies the address of the TFTP or SFTP server. • A.B.C.D—specifies the IP address • WORD—specifies the IPv6 address
filename <*name*>	Specifies the configuration file name.
unit <*unit number*>	Specifies the stack unit number.

The following table describes the **configure network load-on-boot** command variables.

Variable	Definition
load-on-boot *{disable* | *use-bootp* | *use-config}*	Specifies the setting to automatically load a configuration file when the system starts *disable* disables the automatic loading of the configuration file. *use-bootp* specifies loading the ASCII configuration file at startup and using BootP to obtain values for the TFTP or SFTP address and file name. *use-config* specifies loading the ASCII configuration file at startup and using the locally configured values for the TFTP or SFTP address and file name. If you omit the variables, the system immediately downloads and runs the ASCII configuration file.

ACLI pipe filter functions

This section provides the supported pipe (|) filter functions.

Count filter

This filter counts the number of lines in the output of a command.

Syntax

```
<ACLI command> | count
```

Example

```
#show running-config | count
```

```
Count: 100 lines
```

Display output matching a pattern

The match filter displays only the output lines that match the given pattern.

Syntax

```
<ACLI command> | match <pattern> [field <number>] [ignore-case] [header
<number>]
```

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Examples

```
#show interfaces | match 1000 header 3
              Status                    Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
9          Enable  Up   Up   Enabled  Enabled     1000Mbps Full   Asymm
```

```
#show interfaces | match disabled field 5 ignore-case
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
11         Enable  Down Down Disabled Enabled
```

Ignore output that matches a pattern

The ignore filter displays only the output lines that do not match the given pattern. The lines matching the pattern are discarded.

Syntax

```
<ACLI command> | except <pattern> [field <number>] [ignore-case] [header
<number>]
```

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Example

```
#show interfaces | except down ignore-case header 3
              Status                    Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
9          Enable  Up   Up   Enabled  Enabled     1000Mbps Full   Asymm
```

Display output from the first match of a pattern

The find filter displays the output of a command starting from the first line that matches the given pattern.

Syntax

```
<ACLI command> | find <pattern> [field <number>] [ignore-case] [header
<number>]
```

Parameter	Description
pattern	Specifies the regular expression to be matched against each line of output. Quotations are required if the parameter contains spaces.
field <number>	Specifies the field in each line to be matched against the pattern. Fields are separated by white spaces and are counted starting with 1 for the left-most field.
ignore-case	Specifies letters to be matched in the pattern regardless of case.
header <number>	Specifies a number of lines from the start of the output to be displayed unchanged before trying to match the pattern. Useful to keep the header of a table intact.

Example

```
#show interfaces | find 47 header 3
              Status                     Auto                         Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
47         Enable  Down Down Enabled  Enabled
48         Enable  Down Down Enabled  Enabled
49         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
50         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
51         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
52         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
```

Do not paginate output of a single command

The no-more command filter temporarily disables pagination for the output of an ACLI command. When the lines of output exceed the terminal length, you are not prompted to continue or to quit but the entire output of the command continues to be displayed. The effect is similar to setting terminal length 0 but only for the current command.

Example

```
#show interfaces | no-more
```

Display only the first few lines of output

The head filter limits the output of a command to the first few lines. If a number is not specified then the first 10 lines are shown.

Syntax

```
<ACLI command> | head [<number>]
```

Parameter	Description
<number>	Specifies the number of lines to keep from the beginning of the output.

Example

```
#show interfaces | head
              Status                  Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation  Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Up   Up   Disabled Enabled     1000Mbps Full   Asymm
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
```

Display only the last few lines of output

The tail filter limits the output of a command to the last few lines. If a number is not specified, then the last 10 lines are shown.

Syntax

```
<ACLI command> | tail {[<number>] | from-line <number> } [header
<number>]
```

Parameter	Description
<number>	Specifies the number of lines to keep from the end of the output.
from-line <number>	Specifies the line from which to start the output.
[header]	Same description as for the other commands which allow it.

Example

```
#show interfaces | tail 3
50         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
51         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
52         Enable  Down Down Enabled  Disabled    10Gbps   Full   Asymm
```

Regular expressions

Match, except, and find filters require a pattern parameter, which is a regular expression.

Pattern parameter	Description
regular expression	Zero or more branches separated by the pipe symbol ‘|’ It matches anything that matches one of the branches.
branch	Zero or more pieces, concatenated. For instance, it matches a match for the first, followed by a match for the second.
piece	An atom possibly followed by `*', `+', or `?'. An atom followed by `*' matches a sequence of 0 or more matches of the atom. An atom followed by `+' matches a sequence of 1 or more matches of the atom. An atom followed by `?' matches a match of the atom, or the null string.
atom	A regular expression in parentheses (matching a match for the regular expression), a range, `.' (matching any single character), `^' (matching the null string at the beginning of the input string), `$' (matching the null string at the end of the input string), a `\' followed by a single character (matching that

Table continues…

Pattern parameter	Description
	character), or a single character with no other significance (matching that character).
range	A sequence of characters enclosed in `[ ]'. It normally matches any single character from the sequence. If the sequence begins with `^', it matches any single character not from the rest of the sequence. If two characters in the sequence are separated by `-', this is shorthand for the full list of ASCII characters between them (for example, `[0-9]' matches any decimal digit). To include a literal `]' in the sequence, make it the first character (following a possible `^'). To include a literal `-', make it the first or last character.
	If the pattern includes white spaces then it must be enclosed in quotation marks.
	To match characters which have a special meaning – one of *.+?^$()[]\ – they must be escaped. They must be preceded by a single backslash if the pattern is not in quotation marks and by double backslash if the pattern is enclosed in quotes.

Regular expression examples

Regular expression	Description
est	Matches a string containing “est”. For example, “testing”.
A(d+)r	Matches a string containing an ‘A’ followed by at least one ‘d’ followed by ‘r’. For example, “Address”.
^1	Matches a ‘1’ only at the beginning of a line.
192\.[0-9]+\.[0-9]+\.[0-9]+	Matches a string representing a valid IPv4 address starting with 192.
“192\\.[0-9]+\\.[0-9]+\\.[0-9]+”	Matches a string representing a valid IPv4 address starting with 192 when the pattern is enclosed in quotes. The un-escaped ‘.’ means “any single character” which would make the regular expression accept invalid addresses as well.

Viewing USB files

About this task

Use this procedure to display configuration files stored on a USB device in a unit in a stack.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Enter `show usb-files`.

Example

The following is an output example for the `show usb-files` command.

```
Switch#show usb-files
USB file list - Stand-alone
Listing Directory USB_BULK:
657 Feb 17 2009 IP.CFG
```

```
6217432 Mar 3 2009 4000_53044.img
1589514 Feb 25 2009 4000_5303.bin
2048 Mar 4 2009 ABC/
```

Viewing USB host port information

About this task

Use this procedure to display the USB host port information for a unit in a stack.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Enter `show usb-host-port [unit <1-8>]`.

Example

The following is an output example for the `show usb-host-port` command.

```
Switch(config)#show usb-host-port
USB Host Port Info - Stand-alone Enabled
----------------------------------------
  Vendor Info       : Imation
  Product ID        : Flash Drive
  Product Revision : 1.00
  Number of Blocks : 1974271
  Bytes per Block   : 512
  Total Capacity    : 1010826752
```

Enterprise Device Manager configuration files

This section describes how to use Enterprise Device Manager (EDM) to store and retrieve configuration files.

Using EDM, you can :

- Store the current ASCII switch configuration file on a TFTP or SFTP server or a USB storage device
- Retrieve an ASCII configuration file from a TFTP or SFTP server or USB storage device to apply to a switch
- Store or retrieve a binary configuration file
- Manually save the current configuration to flash memory

You can check file upload transfer status of ASCII configuration files in the ScriptLastStatusChange field on the **Edit** > **File System** > **Ascii Config Script Files** tab. During upload transfer, the status is `manualUploadInProgress`. To check changes to file transfer status, click **Refresh**. After the file transfer is complete the status displays as either `manualUploadPassed` or `manualUploadFailed`.

You can check file download transfer status of ASCII configuration files in the ScriptLastStatusChange field on the **Ascii Config Script Files** tab. During download transfer, the status is `manualDownloadInProgress`. To check changes to file transfer status, click **Refresh**. After the file transfer is complete, the status displays as either `manualDownloadPassed` or `manualDownloadFailed`.

You can also designate an ASCII configuration file to download automatically at switch startup.

To control which ASCII configuration files load automatically, at switch startup use the fields in the table on the **Edit** > **File System** > **Ascii Config Script Files**.

The **Ascii Config Script Files** table provides a way to control which ASCII configuration files are loaded, and in which order, because you can designate the path to an ASCII configuration file, a boot priority value, and a script index priority for each entry in the table.

Depending on which script source you designate for an entry, the system uses the designated paths in the Ascii Config Script Files table in one of the following ways:

- The system uses BootP to download the designated ASCII configuration file from the network, according to the specified IP address and file name.
- The system downloads the designated ASCII configuration file from a TFTP or SFTP server, according to the specified IP address and file name.
- The system downloads the ASCII configuration file from a USB device, according to the specified file name.

In the **boot priority** column on the Ascii Config Script Files tab, if you designate a non-zero boot priority value for any but the first row, the switch attempts to load the configuration file at startup. The first entry in the configuration files table is assigned a fixed boot priority value of 0 and it is not available to load at startup.

The switch attempts to load each ASCII configuration file with a non-zero priority value, in ascending order, until a script file loads successfully. If ASCII configuration file boot priority values are equal, the switch attempts to load the configuration files according to their script index order.

In the **Script Source** column in the Ascii Config Script Files table, if you designate a USB device in a stand-alone switch as the load-on-boot path to the ASCII configuration file, the switch downloads the specified configuration file from the USB port of the switch.

If you designate a USB device in a stack unit as the load-on-boot path to the ASCII configuration file entry, the system downloads the specified configuration file from the USB port of the designated unit or, if no unit is designated, from the USB port of the base unit.

If the system cannot download the configuration file, or if the script does not execute successfully, the script operational status changes to `autoDownloadFailed` and the system downloads the next entry in the table.

When the configuration file downloads and executes without errors, the operational status for the entry changes to `autoDownloadPassed`.

ASCII and binary configuration file procedures

Perform the procedures in this section to use EDM to manage ASCII and binary configuration files. For more information about fields on the **Config/ImageDiag file** tab, used to manage binary configuration files, see Config Image Diag file tab field descriptions job aid on page 68.

Procedures for USB devices apply only to switch models equipped with USB ports.

Storing current ASCII configuration on a TFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.
3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the TFTP server address and the configuration file name in the following format:

   ```
   tftp://<ip address>/<filename>
   ```

   The entry is limited to a maximum of 327 characters.
5. Double-click the **ScriptManual** field and then click **Upload**.
6. On the toolbar, click **Apply**.

Storing current ASCII configuration on a SFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.
3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the SFTP server address and the configuration file name in the following format:

   ```
   sftp://<ip address>/<filename>
   ```

   The entry is limited to a maximum of 327 characters.
5. Double-click the **ScriptManual** field and then click **Upload**.
6. On the toolbar, click **Apply**.

Storing current ASCII configuration on a USB device using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.

3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type:

   `usb://<filename>` to store the configuration file on a USB device in a stand-alone unit

   or

   `usb://<unit number>/<filename>` to store the configuration file on a USB device in a unit in a stack.
5. Double-click the **ScriptManual** field and then click **Upload**.
6. On the toolbar, click **Apply**.

Downloading an ASCII Configuration from a TFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.
3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the TFTP server IP address and configuration file name in the following format:

   ```
   tftp://<ip address>/<filename>
   ```
5. Double-click the **ScriptManual** field and then click **Download**.
6. On the toolbar, click **Apply**.

Downloading an ASCII configuration from a SFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.
3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the SFTP server IP address and configuration file name in the following format:

   ```
   sftp://<ip address>/<filename>
   ```
5. Double-click the **ScriptManual** field and then click **Download**.
6. On the toolbar, click **Apply**.

Downloading an ASCII configuration from a USB device using EDM

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. Click **File System**.

3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the configuration file name in the following format:

   `usb://<filename>` for a USB device in a standalone unit

   or

   `usb://<unit number>/<filename>` for a USB device in a unit in a stack
5. Double-click the **ScriptManual** field, and then click **Download**.
6. On the toolbar, click **Apply**.

Downloading a configuration file automatically using EDM

Procedure

1. From the navigation tree, double-click **Edit**.
2. Click **File System**.
3. Click the **Ascii Config Script Files** tab.
4. Double-click the **ScriptSource** field and type the TFTP server IP address and the configuration file name in the following format:

   `tftp://<ip address>/<filename>`.

   Substitute `usb://<filename>` to retrieve a configuration from a USB device in a stand-alone unit or `usb://<unit number>/<filename>` if the USB device resides in a unit in a stack.

   If you retrieve the configuration file from a BOOTP server, type `bootp://` in the **ScriptSource** field.
5. Double-click the **ScriptBootPriortity** field and type a digit between 1 and 127 for the script priority. Use **0** if you are not using the entry at startup.
6. On the toolbar, click **Apply**.

Storing a binary configuration file on a TFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit**.
2. Click **File System**.
3. Click the **Config/Image/Diag file** tab.
4. In the **TftpServerInetAddressType** dialog box, click the applicable address type button.
5. In the **TftpServerInetAddress** field, enter the TFTP server IP address.
6. In the **BinaryConfigFilename** field, enter the configuration file name.
7. In the **BinaryConfigUnitNumber** field enter the stack unit number or, for a stand-alone switch, enter `0`.

8. In the **Action** box, click **upldConfig**.
9. On the toolbar, click **Apply**.

Storing a binary configuration file on a USB device using EDM

Procedure

1. From the navigation tree, double-click **Edit** .
2. Click **File System**.
3. Click the **Config/Image/Diag file** tab.
4. In the **BinaryConfigFilename** field, enter the configuration file name.
5. In the **BinaryConfigUnitNumber** field enter the stack unit number or, for a stand-alone switch, enter `0`.
6. In the **UsbTargetUnit** field, enter the stack number where the USB device is inserted.
7. In the **Action** field, click **upldConfigtoUsb**.
8. On the toolbar, click **Apply**.

Downloading a binary configuration file from a TFTP server using EDM

Procedure

1. From the navigation tree, double-click **Edit**.
2. Click **File System**.
3. Click the **Config/Image/Diag file** tab.
4. In the **TftpServerInetAddress** field, enter the TFTP server IP address.
5. In the **BinaryConfigFilename** field, enter the configuration file name.
6. In the **BinaryConfigUnitNumber** field, enter the stack unit number, or for a stand-alone switch, enter `0`.
7. In the **Action** field, click **dnldConfig**.
8. On the toolbar, click **Apply**.

Downloading a binary configuration file from a USB device using EDM

Procedure

1. From the navigation tree, double-click **Edit**.
2. Click **File System**.
3. Click the **Config/Image/Diag file** tab.
4. In the **BinaryConfigFilename** field, enter the configuration file name.
5. In the **BinaryConfigUnitNumber** field, enter the stack unit number, or for a stand-alone switch, enter `0`.

6. In the **UsbTargetUnit** field, enter the stack unit number where the USB resides.
7. In the **Action** field, click **dnldConfigFromUsb**.
8. On the toolbar, click **Apply**.

Saving current configuration to flash memory manually using EDM

Procedure

1. From the navigation tree, double-click **Edit**.
2. Click **File System**.
3. Click the **Save Configuration** tab.
4. Ensure that **AutosavetoNvramEnabled** is not selected.
5. In the **Action** field, click **copyConfigToNvram**.
6. On the toolbar, click **Apply**.
7. On the toolbar, click **Refresh** to check progress.

Job aid—Config/Image/Diag file tab field descriptions

The following table provides information about fields on the Config/Image/Diag file tab.

Field name	Description
TftpServerInetAddressType	Specifies the IP version of the TFTP server address
TftpServerInetAddress	Specifies the TFTP server IP address
BinaryConfigFilename	Specifies the name of the binary configuration file
BinaryConfigUnitNumber	Specifies the unit number of a switch in a stack
ImageFileName	Specifies the software image file name
FWFileName(Diagnostics)	Specifies the diagnostics file name
USBTargetUnit	Specifies the unit number containing the USB port
Action	• **dnldConfigFromUSB**—Downloads a configuration to the switch from a USB device. • **DnldImgIfNewer**—Downloads a new software image to the switch only if it is newer than the current image. • **dnldFw**—Downloads a new diagnostic software image to the switch. • **dnldConfig**—Downloads a configuration file to the switch. • **upldConfigToUsb**—Uploads a configuration file to a USB device. • **dnldImgNoReset**—Downloads a new software image to the switch without a switch reset. • **dnldFwNoReset**—Downloads a new diagnostic software image to the switch without a switch reset.

Table continues…

Field name	Description
	• **upldConfig**—Uploads a configuration file to the switch from a designated location. • **dnldImg**—Downloads a new software image to the switch. • **dnldImgFromUsb**—Downloads a new software image to the switch from a USB device. • **dnldFwFromUsb**—Downloads a new diagnostic software image to the switch from a USB device. • **dnldImgFromSftp**—Downloads a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • **dnldFwFromSftp**—Downloads a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image. • **dnldConfigFromSftp**—Downloads a configuration to the switch from the SFTP server. • **upldConfigToSftp**—Uploads a configuration to the SFTP server. • **dnldImgFromSftpNoReset**—Downloads the agent image from a SFTP server anddoes not reset the switch. • **dnldFwFromSftpNoReset**—Downloads the diagnostic image from a SFTP server and does not reset the switch.
Status	Displays the status of the most recent action since last switch restart.

Displaying USB file information using EDM

About this task

Displays the general information of the files on a USB flash device.

Procedure

1. From the navigation tree, click **Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

Chapter 6: Supported standards and RFCs

Use this chapter as a quick reference for standards and RFCs supported by the switch.

Standards

The standards in the following list are supported on the switch:

- IEEE 802.1X (EAPOL)
- IEEE 802.3 (Ethernet)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.1ab (Link Layer Discovery Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1D (Spanning Tree Protocol)
- IEEE 802.1Q (VLAN Tagging)

RFCs

For more information about networking concepts, protocols, and topologies, consult the following RFCs:

- RFC 768 UDP
- RFC 783 TFTP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet

- RFC 894 IP over Ethernet
- RFC 903 Reverse ARP
- RFC 950 / RFC 791 IP
- RFC 951 BootP
- RFC 958 NTP
- RFC 1058 RIPv1
- RFC 1112 IGMPv1
- RFC 1122 Requirements for Internet hosts
- RFC 1155 SMI
- RFC 1156 MIB for management of TCP/IP
- RFC 1157 SNMP
- RFC 1212 Concise MIB definitions
- RFC 1213 MIB-II
- RFC 1215 SNMP Traps Definition
- RFC 1340 Assigned Numbers
- RFC 1350 TFTP
- RFC 1354 IP Forwarding Table MIB
- RFC 1398 Ethernet MIB
- RFC 1442 SMI for SNMPv2
- RFC 1450 MIB for SNMPv2
- RFC 1493 Bridge MIB
- RFC 1519 Classless Inter-Domain Routing (CIDR)
- RFC 1591 DNS Client
- RFC 1650 Definitions of Managed Objects for Ethernet-like Interfaces
- RFC 1724 / RFC 1389 RIPv2 MIB extensions
- RFC 1769 / RFC 1361 SNTP
- RFC 1886 DNS extensions to support IPv6
- RFC 1908 Coexistence between SNMPv1 & v2
- RFC 1945 HTTP v1.0
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TDP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2096 IP Forwarding Table MIB
- RFC 2131 / RFC 1541 Dynamic Host Configuration Protocol (DHCP)

- RFC 2138 RADIUS Authentication
- RFC 2139 RADIUS Accounting
- RFC 2236 IGMPv2
- RFC 2328 / RFC 2178 / RFC 1583 OSPFv2
- RFC 2453 RIPv2
- RFC 2454 IPv6 UDP MIB
- RFC 2460 IPv6 Specification
- RFC 2461 IPv6 Neighbor Discovery
- RFC 2464 Transmission of IPv6 packets over Ethernet
- RFC 2474 Differentiated Services (DiffServ)
- RFC 2541 Secure Shell protocol architecture
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 Expedited Forwarding PHB Group
- RFC 2616 / RFC 2068 HTTP 1.1
- RFC 2660 HTTPS - Secure Web
- RFC 2665 / RFC 1643 Ethernet MIB
- RFC 2674 Q-BRIDGE-MIB
- RFC 2710 Multicast Listener Discovery version 1 (MLDv1)
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2787 Definitions of Managed Objects for VRRP
- RFC 2819 / RFC 1757 / RFC 1271 RMON
- RFC 2851 Textual Conventions for Internet network addresses
- RFC 2863 / RFC 2233 / RFC 1573 Interfaces Group MIB
- RFC 2865 RADIUS
- RFC 2866 / RFC 2138 RADIUS Accounting
- RFC 2869 RADIUS Extensions—Interim updates
- RFC 2933 IGMP MIB
- RFC 3058 RADIUS Authentication
- RFC 3140 / RFC 2836 Per-Hop Behavior Identification codes
- RFC 3162 IPv6 RADIUS Client
- RFC 3246 Expedited Forwarding Per-Hop Behavior
- RFC 3260 / RFC 2475 Architecture for Differentiated Services
- RFC 3289 DiffServ MIBs
- RFC 3410 / RFC 2570 SNMPv3
- RFC 3411 / RFC 2571 SNMP Frameworks

- RFC 3412 / RFC 2572 SNMP Message Processing
- RFC 3413 / RFC 2573 SNMPv3 Applications
- RFC 3414 / RFC 2574 SNMPv3 USM
- RFC 3415 / RFC 2575 SNMPv3 VACM
- RFC 3416 / RFC 1905 SNMP
- RFC 3417 / RFC 1906 SNMP Transport Mappings
- RFC 3418 / RFC 1907 SNMPv2 MIB
- RFC 3513 IPv6 Addressing Architecture
- RFC 3484 Default Address Selection for IPv6
- RFC 3569 Overview of Source Specific Multicast (SSM)
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 3579 RADIUS support for EAP
- RFC 3584 / RFC 2576 Co-existence of SNMP v1/v2/v3
- RFC 3587 IPv6 Global Unicast Format
- RFC 3596 DNS extensions to support IPv6
- RFC 3621 Power over Ethernet MIB
- RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types
- RFC 3768 / RFC 2338 VRRP
- RFC 3810 Multicast Listener Discovery version 2 (MLDv2)
- RFC 3826 AES for the SNMP User-based Security Model
- RFC 3917 Requirements for IPFIX
- RFC 3954 Netflow Services Export v9
- RFC 3993 DHCP Subscriber-ID sub-option
- RFC 4007 Scoped Address Architecture
- RFC 4022 / RFC 2452 TCP MIB
- RFC 4113 UDP MIB
- RFC 4133 / RFC 2737 / RFC 2037 Entity MIB
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Transition Mechanisms for IPv6 Hosts & Routers
- RFC 4250 SSH Protocol Assigned Numbers
- RFC 4251 SSH Protocol Architecture
- RFC 4252 SSH Authentication Protocol
- RFC 4253 SSH Transport Layer Protocol
- RFC 4254 SSH Connection Protocol
- RFC 4291 IPv6 Addressing Architecture

- RFC 4293 IPv6 MIB
- RFC 4344 SSH Transport layer Encryption Modes
- RFC 4345 Improved Arcfour Modes for SSH
- RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
- RFC 4432 SSHv2 RSA
- RFC 4443 / RFC 2463 ICMPv6 for IPv6
- RFC 4541 Considerations for IGMP and MLD snooping switches
- RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification
- RFC 4604 / RFC 3376 IGMPv3
- RFC 4673 RADIUS Dynamic Authorization Server MIB
- RFC 4675 RADIUS Attributes for VLAN and Priority Support
- RFC 4716 SSH Public Key File Format
- RFC 4750 / RFC 1850 / RFC 1253 OSPF v2 MIB
- RFC 4789 SNMP over IEEE 802 Networks
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 / RFC 2462 IPv6 Stateless Address Auto-Configuration
- RFC 5010 / RFC 3046 DHCP Relay Agent Information Option 82
- RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for Exchange of IP Traffic
- RFC 5176 / RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 5186 IGMPv3/MLDv2 and Multicast Routing Interaction
- RFC 5905 / RFC 4330 / RFC 1305 NTPv4
- RFC 6329 IS-IS Extensions Supporting Shortest Path Bridging

Chapter 7: ACLI quick reference

This chapter provides a quick reference for frequently used ACLI tasks.

For more information about using ACLI, see User interface fundamentals on page 16.

For more information about detailed configuration, see the function-specific configuration documents for this product. For the list of documents, see *Documentation Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205–101.

Connect to the switch

Two options you can use to connect to the switch are:

- remote
- console

The following table lists the access method for three types of connection.

Secure Shell (SSH) enabled	SSH not enabled	Console access available
Remote access	Telnet access	Normal console connection access

Start ACLI from the main menu

To start a configuration using ACLI, choose `Command Line Interface` from the main menu.

At the prompt, use the commands in the following table.

Command	Purpose
`enable`	Enter configuration mode
`config t`	Start configuration

Use the factory default configuration

Use the commands in the following table to restart the switch using the factory default configuration.

Command	Purpose
`exit`	Exit the configuration mode.
`boot default`	Return a switch, or switches, to factory default configuration.
`restore factory-default [-y]`	Return a switch, or switches, to factory default configuration where [-y] instructs the switch not to prompt for confirmation.

Configure the management IP address

Use the commands in the following table to configure and verify the management IP address.

Command	Purpose
`ip address` *<IP>* `netmask` *<mask>*	Set the management IP and mask.
`ip default-gateway` *<default gateway IP>*	Set the default gateway IP address.
`ping` *<default gateway IP>*	Verify connectivity.
`ping` *[<ipv6address> | <Hostname or A.B.C.D>] [source <WORD>]*	Verify connectivity between a source IPv4 address and another interface.
`show ip`	Verify configuration.

Note:

To dynamically change the switch IP address, you must include the network mask in the command. If you currently have active management IP connections, then changing the management IP address results in disconnecting those sessions. If Layer 3 is enabled, and you use a circuitless IP address, you can configure up to four circuitless IP addresses on the switch or stack.

Configure Simple Network Management Protocol (SNMP)

Use the commands in the following table to configure SNMP.

Command	Purpose
`snmp-server enable`	Enable SNMP (the default setting is disabled).
`snmp-server authentication-trap enable`	Enable authentication traps.

Table continues…

Command	Purpose
`snmp-server community ro`	Set the read-only community name (requirement: enter community string twice).
`snmp-server community rw`	Set the read-write community name (requirement: enter community string twice).
`snmp-server contact` *`<contact information>`*	Set contact information.
`disable`	Disable SNMP access.
`enable`	Enable SNMP access.
`snmp-server location "`*`<Building and Closet number>"`*	Set building name and closet information.
`snmp-server name "`*`<switch IP address>`*`"`	Maintain coherent Syslog messages.
`snmp-server host` *`<host IP> <community>`*	Set IP address of Jscan trap receiver.
`show sys-info`	Verify configuration.
`show snmp host`	Verify configuration.

Configure Network Time Protocol (NTP)

Use the commands in the following table to configure NTP and verify the configuration.

Command	Purpose
`clock source ntp`	Set the clock source to NTP.
`default clock source`	Reset clock source to the default, SNTP.
`clock sync-rtc-with-ntp enable`	Synchronize RTC with NTP where available.
`no clock sync-rtc-with-ntp enable`	Desynchronize RTC with NTP.
`default clock sync-rtc-with-ntp enable`	Set RTC to default; no synchronization with NTP or SNTP.
`ntp [interval]`	Enable NTP globally and specify the interval (in minutes) between NTP updates.
`default ntp [interval]`	Set NTP globally to default (disabled) with the default interval of 15 minutes.
`ntp authentication-key <1-2147483647> <word>`	Create authentication keys for MD5 authentication (maximum of 10).
`no ntp authentication-key [ <1-2147483647> ]`	Delete authentication keys for MD5 authentication.
`default ntp [interval]`	Set authentication keys to the default value.
`ntp server [ <A.B.C.D> | [<IPv6_address>]`	Add the NTP server entries.

Table continues…

Command	Purpose
`default ntp server [ <A.B.C.D> | [<IPv6_address>]`	Set the NTP server entries to the default value.
`no ntp server [ <A.B.C.D> | <IPv6_address>]`	Delete an NTP server.
`show ntp`	Display the NTP global settings.
`show ntp key`	Display the NTP authentication keys.
`show ntp server`	Display the NTP server list and settings.
`show ntp statistics`	Display the NTP statistics such as NTP server IP address, stratum, version, sync status, reachability, root delay, access attempts, server sync statistics, and server fail statistics.

Configure VLANs and tagged uplinks

Use the commands in the following table to configure VLANs and tagged uplinks.

Command	Purpose
`Vlan configcontrol automatic`	Automatically deletes old VLANs and updates PVID when a VLAN is added to an untagged port (setting appears at the bottom of the VLAN configuration information).
`vlan ports` *`<uplink port>`* `tagging tagall`	Enables tagging on the uplink.
`vlan ports` *`<uplink port>`* `filter-untagged-frame enable`	Discards the untagged frames.
`vlan ports ALL filter-unregistered-frame disable`	Breaks STP for VoIP.
`vlan create` *`<VID>`* `type port`	Creates the port based VLAN and assign the 802.1q identifier.
`vlan name` *`<VID> <name>`*	Names the VLAN according to conventions.
`vlan members add` *`<VID> <port listing>`*	Adds ports to appropriate VLANs.
`vlan mgmt` *`<VID>`*	Sets the management VLAN.
`vlan members remove 1 ALL`	Removes all ports from VLAN 1.
`vlan ports` *`<uplink port>`* `pvid` *`<VID>`*	Sets the PVID on the uplink.
`show vlan`	Verifies the VLAN configuration.
`show vlan interface info`	Verifies configuration of PVID and port type.
`show vlan interface verbose` *`<LINE>`*	Verifies configuration of VLAN, PVID and port type.

Configure Internet Group Management Protocol (IGMP)

Use the commands in the following table to configure IGMP.

Command	Purpose
`[no][default]ip igmp`	Configure/restore/clear/delete IGMP settings per VLAN.
`ip igmp flush vlan <1-4094>[grp-member] [mrouter]`	Flush the group member or IGMP Mrouter on selected VLAN interface.
`[default] ip igmp last-member-query-interval <0-255>`	Configure/restore default last member query interval per VLAN.
`[no][default] ip igmp mrouter <LINE>`	Configure/remove multicast forwarding ports per VLAN.
`[no][default] ip igmp proxy`	Enable/disable IGMP proxy per VLAN.
`[default] ip igmp query-max-response <0-255>`	Configure/restore to default maximum response time in query message (1/10 of a second) per VLAN.
`[default] ip igmp query-interval<1-65535>`	Configure/restore to default query interval time per VLAN, in seconds.
`[default] igmp robust-value <2-255>`	Configure/restore to default robustness variable per VLAN.
`[no][default] ip igmp router—alert`	Configure to accept/ignore IGMP packets with router-alert option in IP header, per VLAN.
`[no][default] ip igmp snooping`	Enable/disable IGMP snooping per VLAN.
`[no][default] ip igmp send-query`	Enable IGMP send query.
`[no][default] ip igmp snoop-querier-addr <A.B.C.D>`	Configures the address of the IGMP snoop querier.
`ip igmp version <1-3>`	Set/restore to default IGMP version.
`show ip igmp cache`	Display IGMP cache details.
`show ip igmp group count`	Display the count of entries.
`show ip igmp group count group <A.B.C.D>`	Display the count of entries for the specified group.
`show ip igmp group count member-subnet <A.B.C.D/<0-32>>`	Display the count of entries for the specified member subnet.
`show ip igmp group group <A.B.C.D>`	Display the IGMP group details for the specified group.
`show ip igmp group member-subnet <A.B.C.D>/<0-32>`	Display the IGMP group details for the specified member subnet.
`show ip igmp group member-subnet <A.B.C.D>/<0-32> group <A.B.C.D>`	Display the IGMP group details for the specified member subnet from the selected group.
`show ip igmp group-ext`	Display the IGMP group extended details.

Table continues…

Command	Purpose
`show ip igmp group-ext count`	Display the count of entries for IGMP group extended details.
`show ip igmp group-ext group <A.B.C.D>`	Display the IGMP group extended details for the selected group.
`show ip igmp group-ext member-subnet<A.B.C.D/<0-32>>`	Display the IGMP group extended details for the selected member subnet.
`show ip igmp group-ext source <A.B.C.D>`	Display the IGMP group extended details for the selected source address.
`show ip igmp interface`	Display IGMP interface information.
`show ip igmp interface vlan <1-4094>`	Display IGMP interface information for the selected VLAN.
`show ip igmp router-alert`	Display router-alert settings.
`show ip igmp router-alert vlan <1-4094>`	Display router-alert settings for the selected VLAN.
`show ip igmp snooping`	Display IGMP snooping information.
`vlan igmp <VID> snooping enable`	Enable IGMP snooping on each appropriate VLAN.
`vlan igmp <VID> proxy enable`	Enable IGMP proxy on each appropriate VLAN.
`show vlan igmp <VID>`	Show IGMP information for each appropriate VLAN.

Configure Multicast Listener Discovery (MLD) snooping

Multicast Listener Discovery (MLD) snooping is an IPv6 multicast constraining mechanism running on Layer 2 devices. When MLD snooping is enabled on a VLAN, Ethernet Routing Switch examines the MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. Based on the learning, the switch forwards multicast traffic only to those interfaces in the VLAN that are connected to the interested receivers, instead of flooding traffic to all the interfaces.

Use the commands in the following table to configure MLD.

Command	Purpose
`[default] [no] ipv6 mld snooping enable`	Enable/restore/delete MLD snooping settings on VLAN.
`[default] ipv6 mld snooping last-memb-query-int <0-255>`	Configure/restore default last member query interval for each VLAN.
`[no] [default] ipv6 mld snooping mrouter LINE`	Configure/remove multicast forwarding ports for each VLAN.
`[default] ipv6 mld snooping query-interval <1-65535>`	Configure/restore to default query interval time for each VLAN, in seconds.

Table continues…

Command	Purpose
`[default] ipv6 mld snooping robust-value <2-255>`	Configure/restore to default robustness variable for each VLAN.
`show ipv6 mld snooping [interface vlan <1-4094>]`	Display MLD snooping interface information for the selected VLAN.
`show ipv6 mld snooping`	Display MLD snooping information.
`show ipv6 mld-cache interface [vlan <1-4094>]`	Display MLD cache information.
`show ipv6 mld group [interface vlan <1-4094>]`	Display MLD group information.

For more information about the feature and configuration, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.

Configure a port

Use the commands in the following table to configure a port.

Command	Purpose
`interface Ethernet<end-user port list>`	Enter configuration mode at the interface level where you can configure multiple ports, excluding uplink ports, simultaneously.
`auto-negotiation-advertisements 10-full 10-half 100-full 100-half pause-frame`	Set 10/100 ports to advertise only 10Mb/s half duplex and 100Mb/s half duplex.
`default auto-negotiation-advertisement`	Advertise gigabit for gigabit ports because Custom Autonegotiation Advertisements (CANA) is not appropriate for gigabit ports.
`poe poe-shutdown`	Because Power Over Ethernet (PoE) is on by default, use this command to disable PoE on non-PoE ports.
`no poe-shutdown`	Enable PoE for AP ports.
`shutdown [port]`	Disable unused ports.
`spanning-tree learning fast`	Set fast spanning tree learning on access ports.
`name <port name>`	Name uplink ports. If you need dual uplinks, Avaya recommends that you add a second switch, in a stack, and use port 48 of the second switch as the second uplink.
`Exit`	Terminate port configuration.
`interface Ethernet <uplink port>`	Enter configuration mode at the interface level to configure port 48 as an uplink port.

Table continues…

Command	Purpose
`speed auto`	Enable autonegotiate.
`spanning-tree learning <normal or disable>`	Depending on the upstream switch location, set spanning tree to normal or disabled.
`name UP-<Switch IP Address>-<Slot>/<Port>`	Example: UP-128.206.95.254-1/2
`Exit`	Terminate uplink configuration.
`show interfaces all`	Display interface settings.

Configure passwords

Use the commands in the following table to configure ACLI passwords.

Command	Purpose
`cli password serial`	Enable or disable the serial port password.
`cli password telnet`	Enable or disable telnet and web passwords.
`no password security`	Remove password complexity and change frequency restrictions.
`cli password read-only`	Modify the read-only password (you are required to enter the password twice).
`cli password read-write`	Modify the read-write password.
`cli password stack`	Modify stack passwords.
`cli password switch`	Modify stand-alone switch passwords.

Configure Secure Shell (SSH)

Use the commands in the following table to configure SSH.

Command	Purpose
`ssh pass-auth`	Enable password authentication for SSH. To use SSHv2 for switch access, ensure that you use SecureCRT 4.1 or newer, Putty, or Linux SSH.
`ssh`	Enable SSH support.
`show ssh global`	Display SSH settings.
`ssh dsa-auth`	Enable DSA authentication for SSH.
`ssh rsa-auth`	Enable RSA authentication for SSH.

Table continues…

Command	Purpose
`ssh dsa-host-key`	Generate new SSH DSA host key.
`ssh rsa-host-key`	Generate new SSH RSA host key.
`ssh secure`	Enable SSH secure mode. Enabling SSH secure mode cuts off all remote access. Telnet, SNMP and web are disabled.

Configure Telnet

To disable Telnet access, use the following command.

`telnet-access disable`.

Configure Simple Network Time Protocol (SNTP)

Use the commands in the following table to configure SNTP.

Command	Purpose
`sntp server {primary address <A.B.C.D> <WORD> | secondary address <A.B.C.D> <WORD>}`	Set the SNTP server address. *<A.B.C.D>* is the IPv4 address of the SNTP server in decimal notation. *<WORD>* is the primary server IPV6 address—maximum 45 characters.
`sntp enable`	Enable SNTP.
`show sntp`	Display SNTP settings. The SNTP default setting is Greenwich Mean Time (GMT).
`sync-interval`	Set the SNTP resynchronization interval.
`sync-now`	Force the immediate SNTP synchronization.

Configure log settings

Use the commands in the following table to configure log settings.

Command	Purpose
`logging volatile overwrite`	Allow the log to overwrite log from the beginning when the buffer is full.

Table continues…

Command	Purpose
`logging remote address` *<A.B.C.D> <WORD>*	*<A.B.C.D.>* is the IP address of the remote syslog server. *<WORD>* is the remote host IPv6 address—maximum 45 characters.
`logging remote level informational`	Log all events.
`logging remote enable`	Enable syslogging.
`logging remote secondary-address` *<A.B.C.D> <WORD>*	*<A.B.C.D.>* is the IP address of the remote syslog server. *<WORD>* is the remote host IPv6 address—maximum 45 characters. **Note:** The configuration of the secondary address is independent of the configuration of the first address (logging remote address command); that is, you can configure the secondary address without configuring the first address.

Configure Secure Socket Layer (SSL)

Use the commands in the following table to configure SSL.

Command	Purpose
`ssl certificate`	Create a certificate on the next startup. For switches that include a secure web server, Avaya recommends that you replace the generic certificate with a new certificate generated by the **`ssl certificate`** command.
`ssl`	Enable SSL server.
`ssl reset`	Reset the SSL server. When SSL is enabled: existing SSL connections are closed. The SSL server is restarted and initialized with the certificate that is stored in the NVRAM. When SSL is not enabled: existing non-secure connections are closed, the server is restarted, and non-secure operation resumes.
`show ssl`	Display SSL settings.

Configure access control

Use the commands in the following table to configure access control.

Command	Purpose
`ipmgr source-ip 1 <trusted net> mask <mask>`	Enable management from the trusted net.
`ipmgr source-ip 2 <trusted net2> mask <mask>`	Enable management from trusted net 2.
`ipmgr source-ip <1-50>`	Select address or mask pair.
`ipmgr source-ip <51-100> <WORD>`	Select IPv6 address or prefix where *WORD* is the IPv6 address or prefix from which connections are allowed.
`show ipmgr`	Display access control configuration.

Check a configuration

To display the switch configuration enter the following command.

```
show running-config.
```

Configure First Hop Security

The enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers. IPv6 First Hop Security (FHS) aids in improving the local network security by employing a number of mitigation techniques.

Use the commands in the following table to configure FHS in Global Configuration mode.

Command	Purpose
`ipv6 fhs enable`	Enables First Hop Security globally. FHS must be enabled for RA-guard and DHCPv6-guard to become operational.
`[no] [default] ipv6 fhs enable`	Disables FHS globally.
`ipv6 fhs ipv6-access-list <ip-access-list-name> <ip-prefix>/<ip-mask-length> [ge <ip-mask- length>] [le <ip-mask-length>] [ mode <allow | deny>]`	Creates the FHS IP access list or adds IP prefixes to the existing IP access list.

Table continues…

Command	Purpose
`[no] [default] ipv6 fhs ipv6-access-list <ip-access-list-name> [<ip-prefix>/<ip-mask-length>]`	Deletes the FHS IP access list or deletes a particular IP prefix from the IP access list.
`ipv6 fhs mac-access-list <mac-access-list-name> <MAC-Address> [ mode <allow | deny>]`	Creates FHS MAC access list or adds a MAC address to the existing MAC access list.
`[no] [default] ipv6 fhs mac-aacess-list <mac-access-list-name> [<MAC-Address>]`	Deletes the FHS MAC access list or a particular MAC entry from the MAC access list.

Use the commands in the following table to display FHS.

Command	Purpose
`show ipv6 fhs status`	Displays the global FHS status; also displays RA-guard, DHCPv6-guard, and ND-inspection status
`show ipv6 fhs capture-policy [interface <port-number>]`	Displays the DHCPv6 or RA-guard configured policy name, and DHCPv6, RA-guard or ND-inspection statistic information such as the number of DHCPv6 or RA packets received and the number of DHCPv6 or RA packets dropped.
`show ipv6 fhs ipv6-access-list [<access-list-name>]`	Displays all the configured IPv6 access lists in the system.
`show ipv6 fhs mac-access-list [<access-list-name>]`	Displays all the configured MAC access lists in the system.
`show running-config [verbose] module ipv6-fhs`	Displays the FHS running configuration. This command is available on base unit (BU) and non base unit (NBU).

For more information about the feature and configuration, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Configure DHCPv6–guard policy

Dynamic Host Configuration Protocol version 6 (DHCPv6)–guard provides Layer 2 security to the DHCPv6 clients by protecting them against rogue DHCPv6 servers. DHCPv6–guard ensures that the Layer 2 device filters DHCPv6 messages targeted to the DHCPv6 clients. The basic filtering criterion is that the Layer 2 device discards the DHCPv6 messages if they are not received on a specified Layer 2 device port.

Use the commands in the following table to configure DHCPv6–guard policy in Global Configuration mode.

Command	Purpose
`ipv6 dhcp guard enable`	Enables the DHCPv6-guard globally.
`no ipv6 dhcp guard enable`	Disables the DHCPv6-guard globally.
`ipv6 dhcp guard policy` *`<policy-name>`*	Creates, configures, or modifies the DHCPv6-guard policy. This command also enables the DHCPv6-guard configuration mode.
`[no] [default] ipv6 dhcp guard policy` *`<policy-name>`*	Deletes or disables the DHCPv6-guard policy.
`ipv6 dhcp guard clear stats [`*`<port-number>`*`]`	Clears the DHCPv6-guard statistics. If port-number is provided, then only that port's statistics are cleared.

Use the commands in the following table to configure DHCPv6–guard policy in DHCP-guard mode.

Command	Purpose
`device-role {client | server}`	Enables verification of the device role attached to the port.
`match server access-list` *`<ipv6-access-list-name>`*	Enables verification of the sender IPv6 address in the inspected messages from the configured authorized device source access list IPv6 access list name. If the access list is not attached, then this inspection is not done. At the same time, if the list is attached and if it does not match any ip-prefixes in the list, then the DHCPv6 packet is dropped. To change this behavior, add a dummy ip-prefix (0.0.0.0/0) with allow option. This changes the default value from drop to allow.
`[no] [default] match server access-list` *`<ipv6-access-list-name>`*	Removes the sender's IPv6 address-based DHCPv6-guard filtering.
`match reply prefix-list` *`<ipv6-prefix-list-name>`*	Enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If prefix-list is not configured, this check is bypassed. An empty prefix-list is treated as a permit. If the access list is not attached, then this inspection is not done. At the same time, if the list is attached and if it does not match any ip-prefixes in the list, then the DHCPv6 packet is dropped. To change the behavior, add a dummy ip-prefix (0.0.0.0/0) with allow option. This changes the default value from drop to allow.
`[no] [default] match reply prefix-list` *`<ipv6-prefix-list-name>`*	Removes the advertised prefix-based DHCPv6-guard filtering.

Table continues…

Command	Purpose
`preference min limit <0-255>`	Enables verification if the advertised preference (in preference option) is greater than the specified limit. If preference is not specified, this check is bypassed.
`preference max limit <0-255>`	Enables verification if the advertised preference (in preference option) is less than the specified limit. If preference is not specified, this check is bypassed. **Note:** If the minimum and maximum limit values are 0, this preference check is ignored

Use the commands in the following table to configure DHCPv6–guard policy in Interface mode.

Command	Purpose
`ipv6 dhcp guard attach-policy <policy-name>`	Applies the DHCPv6-guard policy on the specific interface. This command is executed on the interface where DHCPv6-guard filter is enabled.
`[no] [default] ipv6 dhcp guard attach-policy <policy-name>`	Detaches the DHCPv6-guard policy on the specific interface.

Use the command in the following table to display DHCPv6–guard policy configuration.

Command	Purpose
`show ipv6 dhcp guard policy <policy-name>`	Displays DHCP-guard policy information for all the configured DHCP-guard policies.

For more information about the feature and configuration, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Configure RA-guard policies

Routed protocols are often susceptible to spoof attacks. Router Advertisements (RA)-guard does not intend to provide a substitute for Secure Neighbor Discovery (SEND)-based solutions. It actually provides complementary solutions in those environments where SEND is not suitable or fully supported by all devices involved.

Use the commands in the following table to configure RA-guard in Global Configuration mode.

Command	Purpose
`ipv6 nd raguard enable`	Enables the RA-guard globally.
`no ipv6 nd raguard enable`	Disables the RA-guard globally.

Table continues…

Command	Purpose
`ipv6 nd raguard policy <policy-name>`	Creates, configures or modifies the RA-guard policy. This command enables the RA-guard configuration mode. It is mandatory to enter the policy-name for creating the RA-guard policy.
`[no] [default] ipv6 nd raguard policy <policy-name>`	Deletes or disables the RA-guard policy.
`ipv6 nd raguard clear stats [<port-number>]`	Clears the RA-guard statistics. If port-number is provided, then only the statistics for that port is cleared. These statistics only show the packets received and dropped at the CPU level.

Use the commands in the following table to configure RA-guard policy in RA-guard mode.

Command	Purpose
`device-role {router | host}`	Enables verification of the device role attached to the port.
`match ipv6 access-list <ipv6-access-list-name>`	Enables verification of the sender IPv6 address in the inspected messages from the configured authorized device source access list IPv6 access list name. If the access list is not attached, then this inspection is not done. At the same time, if the list is attached and if it does not match any ip-prefixes in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix (0::0/0) with allow option. This changes the default value from drop to allow.
`[no] [default] match ipv6 access-list <ipv6-access-list-name>`	Removes the IPv6 address of the sender-based RA-guard filtering.
`match ra prefix-list <ipv6-access-list-name>`	Enables verification of the advertised prefixes in the inspected messages against the configured authorized prefix-list (IPv6 access list name). Inspection is done if the access list is not attached. At the same time, if the list is attached and if it does not match any ip-prefixes in the list, then the RA packet is dropped. To change the behavior, add a dummy ip-prefix (0::0/0) with allow option. This changes the default value from drop to allow.
`[no] [default] match ra prefix-list <ipv6-access-list-name>`	Removes the advertised prefix-based RA-guard filtering.
`match mac-access-list <mac-access-list-name>`	Enables verification of the sender source MAC address against the configured MAC access list. The inspection is not done if the access list is not attached.

Table continues…

Command	Purpose
	At the same time, if the list is attached and if it does not match any MAC address in the list, then the RA packet is dropped. To change the behavior, add a dummy MAC address (0:0:0:0:0:0) to the list with allow option. This changes the default value from drop to allow.
`[no] [default] match mac-access-list <mac-access-list-name>`	Removes the source MAC address-based RA-guard filtering.
`managed-config-flag <none |on | off>`	Enables verification of the managed address configuration flag in the advertised RA packet. By default, the value is none and the check is bypassed.
`hop-limit {maximum | minimum} <0-255>`	Enables verification of the advertised hop count limit. The limit value range is between 0 and 255. By default, the minimum and maximum limit is 0 and for this value, hop-limit check is bypassed.
`router-preference maximum {none | high | low | medium}`	Enables verification of the advertised default router-preference parameter value. It checks if the value is lower than or equal to a specified limit. By default the value is none and for this value, the check is bypassed.

Use the commands in the following table to configure RA-guard policy in the Interface mode.

Command	Purpose
`ipv6 nd raguard attach-policy [<policy-name>]`	Applies the RA-guard policy on the specific interface.
`[no] [default] ipv6 nd raguard attach-policy [<policy-name>]`	Detaches the RA-guard policy on the specific interface.

Perform the commands in the following table to display RA-guard policy.

Command	Purpose
`show ipv6 nd raguard policy [<policy-name>]`	Displays the configured RA-guard policy information.

For more information about the RA-guard feature and configuration, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Configure ND-inspection

The IPv6 Neighbor Discovery (ND) inspection learns and secures bindings for stateless auto configuration addresses in Layer 2 neighbor tables. IPv6 ND-inspection analyzes Neighbor

Discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages without valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

Use the commands in the following table to configure ND-inspection in Global Configuration mode.

Command	Purpose
`ipv6 nd inspection enable`	Enables ND inspection globally.
`[no] [default] ipv6 nd inspection enable`	Disables the ND inspection globally and all the corresponding dynamically-learned Source Binding Table (SBT) entries are also deleted.
`ipv6 neighbor binding vlan <vlan-id> <ipv6-address> interface <interface-type> <port> <mac-address>`	Adds a static entry to the SBT. IPv6 address with 0::0 and LL-MAC with 0:0:0:0:0:0 are not allowed. The static entry replaces the dynamic entry (matching the source IP address). If there is an existing static SBT entry (matching the source IP address) and another static SBT entry is added with the different MAC address or port, those entries are not overwritten. The same SBT entry can be added to a different VLAN
`no ipv6 neighbor binding vlan <vlan-id> <ipv6-address> interface <interface-type> <port> <mac-address>`	Deletes static or dynamic entry from the SBT.
`ipv6 neighbor binding max-entries <1 - 1024>`	Specifies the maximum number of dynamic entries that are allowed to be inserted in the SBT.
`ipv6 neighbor binding clear`	Clears all the dynamically-learned SBT entries. The static SBT entry is not cleared. This clears the learned information such as DHCP-learned information and others.
`default ipv6 neighbor binding max-entries`	Changes the default SBT entry value to 512.
`ipv6 neighbor binding reachable-lifetime [<30 - 86400 seconds> | infinite]`	Specifies the maximum reachable lifetime for a dynamically-learned SBT entry.
`default ipv6 neighbor binding reachable-lifetime`	Changes the reachable lifetime to the default value (300 seconds).
`ipv6 neighbor binding stale-lifetime [< 30 - 86400 seconds> | infinite]`	Specifies the maximum stale lifetime for a dynamically-learned SBT entry.
`default ipv6 neighbor binding stale-lifetime`	Changes the stale lifetime to the default value (86400 seconds).
`ipv6 neighbor binding down-lifetime [<30 - 86400 seconds> | infinite]`	Specifies the maximum down lifetime for a dynamically-learned SBT entry.
`default ipv6 neighbor binding down-lifetime`	Changes the down lifetime to the default value (86400 seconds).

Table continues…

Command	Purpose
`ipv6 nd inspection clear stats [<port-number>]`	Clears the ND-inspection statistics as well as the SBT entry drop status. If the port-number option is given, then only the statistics for that particular port are cleared.
`ipv6 fhs nd inspection stats clear`	Clears ND inspection statistics globally. In this case, it clears the SBT entry overflow statistics.

Use the commands in the following table to configure ND-inspection in Interface mode.

Command	Purpose
`ipv6 nd inspection [dynamic-learning enable]`	Enables the ND inspection on an interface.
`[no] [default] ipv6 nd inspection [dynamic-learning enable]`	Disables the ND inspection on an interface.

Use the commands in the following table to display ND-inspection.

Command	Purpose
`show ipv6 neighbor binding [vlan <vlan-id> | interface <type> <number> | ipv6 <ipv6-address>]`	Displays SBT entries and other timer values.

For more information about the ND-inspection feature and configuration, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Chapter 8: 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

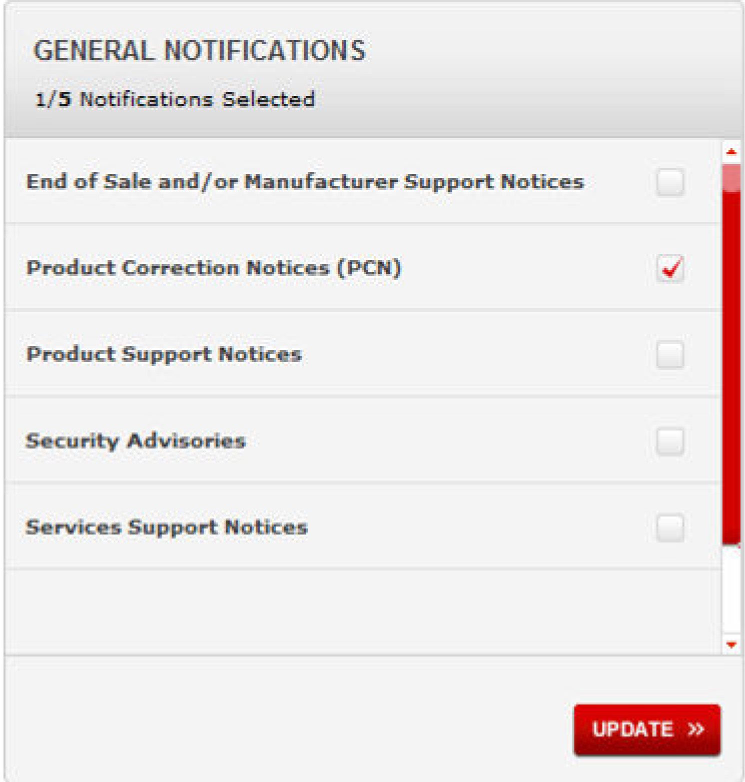
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

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**.

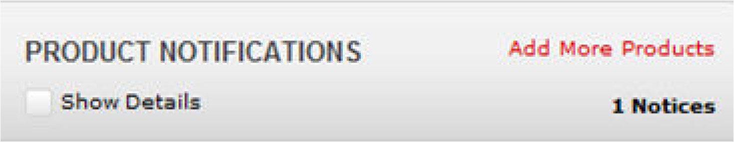


GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices □
- Product Correction Notices (PCN) ☑
- Product Support Notices □
- Security Advisories □
- Services Support Notices □

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

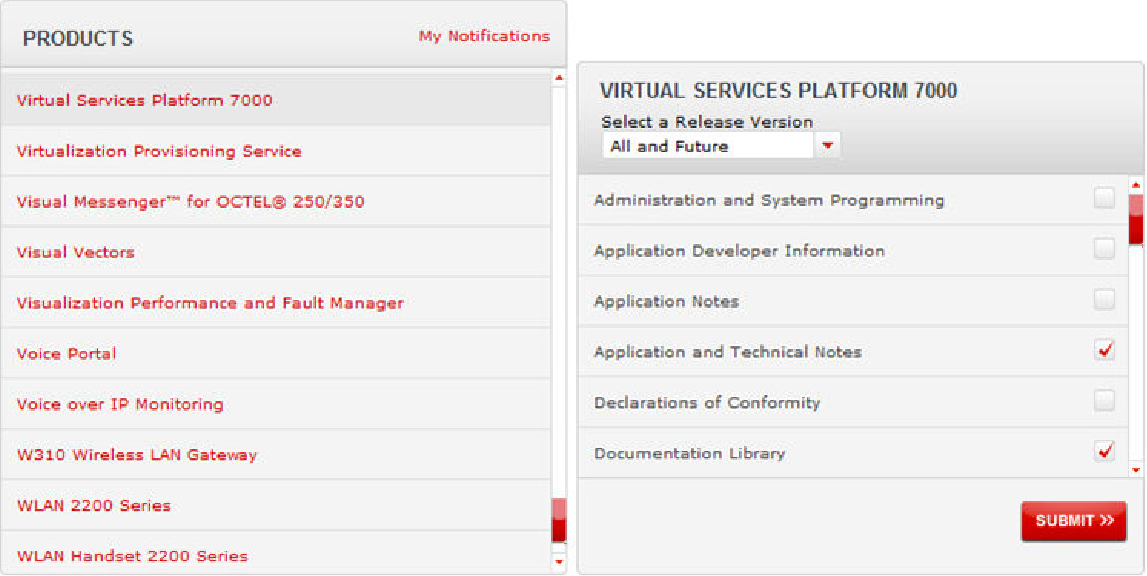


PRODUCT NOTIFICATIONS

□ 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
- 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

VIRTUAL SERVICES PLATFORM 7000

Select a Release Version: All and Future

- Administration and System Programming □
- Application Developer Information □
- Application Notes □
- Application and Technical Notes ☑
- Declarations of Conformity □
- Documentation Library ☑

11. Click **Submit**.