Quick Start Configuration for Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-104
Issue 01.01
November 2013

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

The Quick Start Guide provides basic instructions to install the hardware and perform basic configuration of the Avaya Ethernet Routing Switch 4000 Series Documentation for Release 5.7.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

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

Avaya Mentor videos

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

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

To find videos on the Avaya support site, select the product name, and check the *videos* checkbox to see a list of available videos.

Note:

Videos are not available for all products.

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

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Searching a document 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, for example, ers4000_5.7x.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.

Support

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

Chapter 2: New in this release

This is a new document for Avaya Ethernet Routing Switch 4000 Series Release 5.7.

Chapter 3: Fundamentals

Provisioning follows hardware installation.

The *Quick Start Configuration for Avaya Ethernet Routing Switch 4000 Series*, NN47205–104 includes the minimum, but essential, configuration steps to:

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

More information ships in the box with your new Ethernet Routing Switch 4000, including

- an installation kit
- a foldout poster, *Quick Installation of Avaya Ethernet Routing Switch 4000 Series*, NN47205–304.

For more information about hardware specifications and installation procedures, see *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

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

System connection

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

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

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

- A terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.
- An Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the switch. The other end of the cable must use a connector appropriate to the serial port on your computer or terminal.

You must shield the cable that connects to the console port to comply with emissions regulations and requirements.

System Logon

After the platform boot sequence is complete, a logon prompt appears. The following table shows the default values for logon and password for console and Telnet sessions.

Table 1: Access levels and default logon values

Access level	Description	Default Logon	Default Password
Read-only	Permits view-only configuration and status information. Is equivalent to Simple Network Management Protocol (SNMP) read-only community access.	ro	ro
Read/write	View and change configuration and status information across the switch. You cannot change security and password settings. This access level is equivalent to SNMP read/write community access.	rw	rw

Secure and non-secure protocols

The following table describes the secure and nonsecure protocols that Ethernet Routing Switch 4000 supports.

Table 2: Secure and nonsecure protocols

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
FTP	Disabled	SCP	Disabled
Telnet	Disabled	SSH v1, v2 Avaya recommends that you use SSHv2 instead of SSHv1.	Disabled
SNMPv1, SNMPv2	Enabled	SNMPv3 You must load the DES/AES image on the platform to use SNMPv3. For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.	Enabled
Rlogin	Disabled	Secure SHell (SSH) v1, v2	Disabled
HTTP	Disabled	HTTPS **Important:** Avaya recommends that you take the appropriate security precautions within the network if you use HTTP.	Enabled

Management port

The ERS 4000 series hardware is not equipped with a designated out-of-band (OOB) management port. Use the management port for OOB management when an IP address is assigned to that port. Use the console interface or the in-band switch IP address set from the console terminal through any network port to manage the switch. Before you can use the OOB

management, you must first assign an IP address to the device. Use one of the following three methods to configure the management IP address after logging on:

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

Refer to *chapter 4: Connecting to the switch* for details on connecting a terminal to the console port on the ERS 4000 Series switch.

Password encryption

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

Important:

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

For more information about configuring passwords, see:

Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series (NN47205-102)

Configuring Security on Avaya Ethernet Routing Switch 4000 Series (NN47205-505).

Enterprise Device Manager

Avaya Ethernet Routing Switch 4000 includes Enterprise Device Manager (EDM), an embedded graphical user interface (GUI) that you can use to manage and monitor the platform through a standard Web browser. EDM is embedded into Ethernet Routing Switch software, and the switch operates as a Web server, so you do not require an additional client software. For more information about EDM, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series*, NN47205-102.

If you want 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.

Enterprise Device Manager access

To access EDM, open *http://<deviceip>/login.html* or *https://<deviceip>/login.html* from either Microsoft Internet Explorer versions 8.x and 9.x, or Mozilla Firefox 23.x.

Important:

You must enable the Web server from ACLI to enable HTTP access to EDM. If you want HTTP access to the device, you must also disable the Web server secure-only option. The Web server secure-only option is enabled by default and allows HTTPS access to the device. Take the appropriate security precautions within the network if you use HTTP.

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

Default user name and password

The following table contains the default user name and password that you can use to log on to Ethernet Routing Switch 4000 using EDM. For more information about changing the Ethernet Routing Switch 4000 passwords, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Table 3: EDM default username and password

Username	Password
admin	password

Important:

The default passwords and community strings are documented and well known. Avaya strongly recommends that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Device Physical View

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:

- a stand-alone switch, called a unit
- a switch stack, called a chassis
- a 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, indicating that the object is selected.

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

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

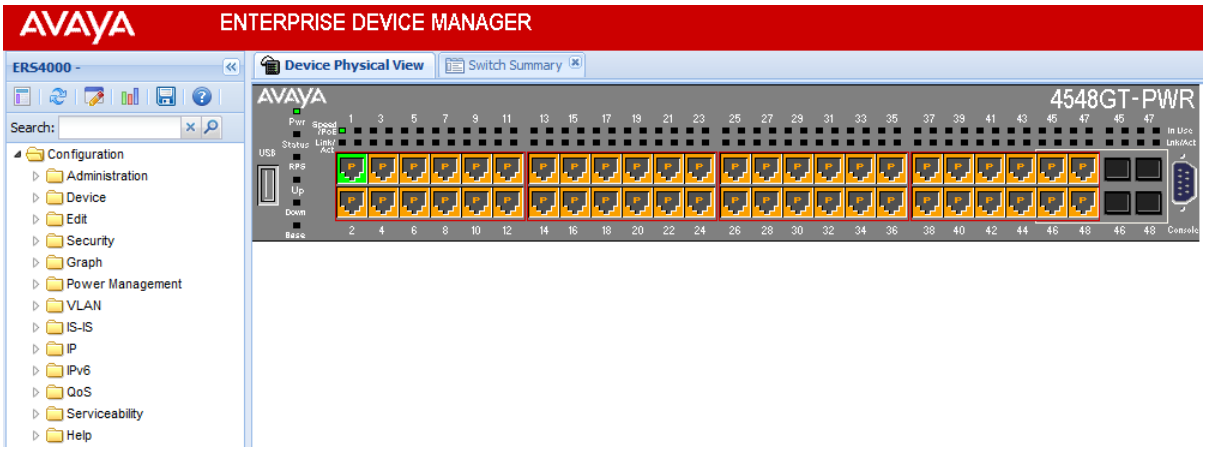

Figure 1: Device Physical View

EDM window

The EDM window contains the following parts:

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

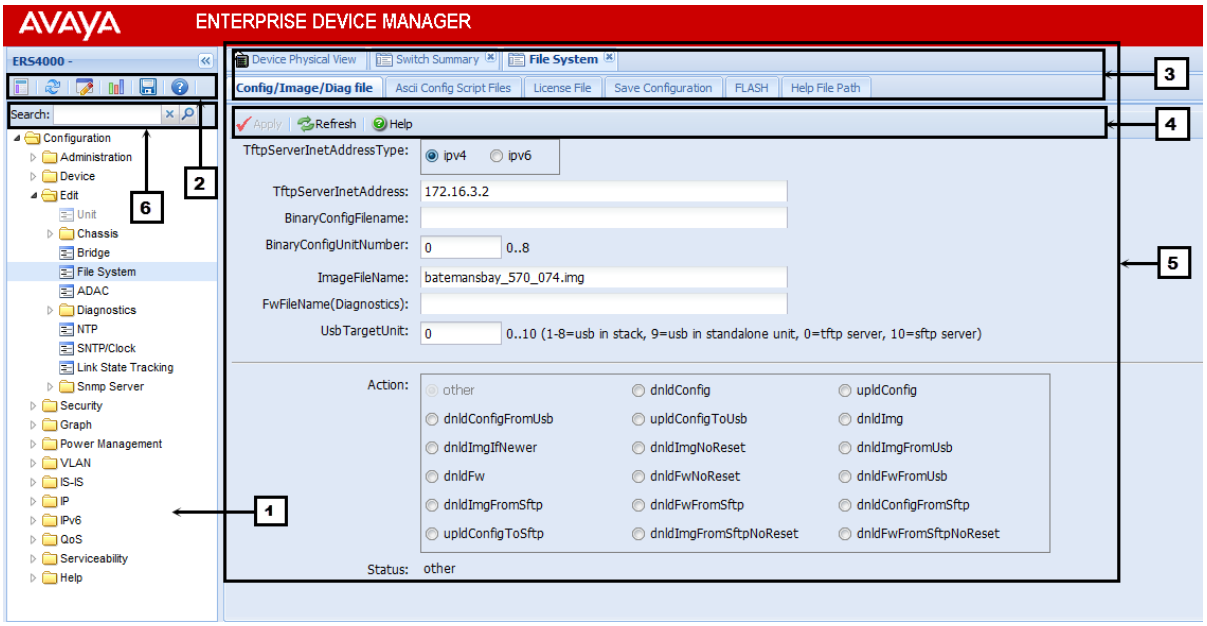

Figure 2: EDM window

Chapter 4: Connecting to the switch

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

Connecting a terminal to the switch

This procedure describes the steps to connect a terminal to the console port on the ERS 4000 Series switch.

Before you begin

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

- Terminal with AC power cord and keyboard. Any terminal or PC with an appropriate terminal emulator can be used as the management station. Refer to *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205–300 for a list of the terminal emulation settings that must be used with any terminal emulation software used to connect to the switch.
- Use the RJ-45 or DB-9 console cable to connect the switch console port to your management terminal.

  Refer to *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205–300 for console port pin-out information. You can use the pin-out information to verify or create a console cable for use with your maintenance terminal.

Procedure

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

```
install
```

The ERS 4000 setup utility banner appears.

8. Enter the IP address at the following prompt:
   ```
   Please provide the in-band IP Address [0.0.0.0]:
   ```
9. Enter the sub-net mask at the following prompt:
   ```
   Please provide the in-band sub-net mask [0.0.0.0]:
   ```
10. Enter the default gateway IP address at the following prompt:
    ```
    Please provide the Default Gateway [0.0.0.0]:
    ```
11. Enter the read only community string at the following prompt:
    ```
    Please provide the Read-Only Community String [**********]:
    ```
12. Confirm the read only community string at the following prompt:
    ```
    Please confirm the Read-Only Community String[**********]:
    ```
13. Enter the read write community string at the following prompt:
    ```
    Please provide the Read-Write Community String [**********]:
    ```
14. Confirm the read write community string at the following prompt:
    ```
    Please confirm the Read-Write Community String[**********]:
    ```
15. Enter the VLAN ID for the Quick Start at the following prompt:
    ```
    Please provide the Quick Start VLAN <1-4094> [1]:
    ```

    Successful completion displays the following message:

    ```
    Basic switch parameters have been configured and saved.
    ```

Example

```
Welcome to the 4548GT-PWR setup utility. You will be requested for information to
initially configure for the switch. When finished the information will be applied
and stored in the switch NVRAM. Once the basic parameters are configured, additional
configuration can proceed using other management interfaces.Press ^C to abort at any
time.
Please provide the in-band IP Address[0.0.0.0]:10.127.232.30
Please provide the in-band sub-net mask[0.0.0.0]:255.255.255.0
Please provide the Default Gateway[0.0.0.0]:10.127.232.1
Please provide the Read-Only Community String[**********]:******
Please confirm the Read-Only Community String[**********]:******
Please provide the Read-Write Community String[**********]:*******
Please confirm the Read-Write Community String[**********]:*******
Please provide the Quick Start VLAN <1-4094> [1]:
Basic switch parameters have now been configured and saved.
```

Important:

Avaya Ethernet Routing Switch 4000 Series only supports the Avaya CLI, the old Bay Stack menu interface is not supported on this product. When the switch is set to factory default parameters, the CLI Quickstart appears which enables you to set default IP information.

Configuring the terminal

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

About this task

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

Important:

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

Procedure

1. Logon to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   `terminal {length <0-132> | width <1-132>}`
3. To display the current serial port information, enter the following command:
   `show terminal`

Variable definitions

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

Table 4: terminal command

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

Chapter 5: Configuring the switch using ACLI

This chapter contains procedures for the initial provisioning of Ethernet Routing Switch 4000. These procedures must be performed when provisioning Ethernet Routing Switch 4000.

Configuring management IP address

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

Before you begin

Ensure to connect the terminal to the switch.

About this task

To set the switch or stack IP address when the switch configuration is not factory default.

Important:

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

Note:

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

Procedure

1. Press `CTRL + Y` after the Avaya banner appears.
2. Enter the Global Configuration command mode in ACLI.

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

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

4. Set the default gateway IP address.
   `ip default-gateway <A.B.C.D>`
5. Save the configuration.
   `save config`

Variable definitions

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

Table 5: ip address command

Variable	Value
<*A.B.C.D*>	Set the management IP address.
netmask <*A.B.C.D*>	Set the subnet mast IP address.

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

Table 6: ip default-gateway command

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

Value of IP address ranges from 0.0.0.0 (no IP address assigned) to 255.255.255.255. For more information on IP addressing and subnet addressing, see *Configuration — IP Routing and Multicast Avaya Ethernet Routing Switch 4000 Series* (NN47205-506).

Configuring BootP on the current instance of the switch or server

About this task

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

Procedure

1. Enable Global Configuration mode in ACLI:
   `enable`

   `configure terminal`

2. At the command prompt, enter the following command:
   `ip bootp server {always | disable | last | default-ip}`

Variable definition

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

Table 7: ip bootp server command

Variable	Value
always | disable | last | default-ip	Specifies when to use BootP: • default-ip—use BootP or the default IP • last—use BootP or the last known address • disable—never use BootP • always—Always use BootP By default, default-ip is selected.

Setting user access limitations using ACLI

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

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

Setting the read-only and read/write passwords

The first step to requiring password authentication when the user logs in to a switch is to edit the password settings. To complete this task, perform the following steps:

1. Access ACLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the **`cli password`** command to change the desired password.

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

   Table 8: cli password parameters on page 28 explains the parameters for the **`cli password`** command.

Table 8: cli password parameters

Parameter	Description
{read-only | read-write}	This parameter specifies if the password change is for read-only access or read/write access.
<password>	If password security is disabled, the length can be 1-15 chars. If password security is enabled, the range for length is 10-15 chars.

3. Press `Enter`.

Enabling and disabling passwords

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

1. Access ACLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the **`cli password`** command to enable the desired password.

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

   The following table explains the parameters for the **`cli password`** command.

Table 9: cli password parameters

Parameter	Description
{telnet | serial}	Specify whether the password is enabled or disabled for Telnet or the console. Telnet and Web access are connected so that enabling or disabling passwords for one enables or disables passwords for the other.
none | local | radius | tacacs	Specifies the password type to modify: • none: disables the password. • local: uses the locally defined password for serial console or Telnet access. • radius: uses RADIUS authentication for serial console or Telnet access.

Parameter	Description
	• tacacs : uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access.

3. Press `Enter`.

Setting user access limitations using EDM

You can use EDM to limit user access by creating and maintaining passwords for Web, Telnet, and Console access.

Related topics:

Configuring the console password using EDM on page 29
Configuring the Web and Telnet password using EDM on page 30

Configuring the console password using EDM

Use the following procedure to configure a password for serial console access to a stack, or standalone switch.

Related topics:

Procedure steps on page 29
Variable definitions on page 30

Procedure steps

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

9. Type the same password for read-write access in the **Re-enter to verify** box.
10. On the toolbar, click **Apply**.

Variable definitions

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

Variable	Value
Console Stack Password Type	Specifies the type of password to use. Values include: • none—disables the password • Local Password— uses the locally defined password for serial console access. • RADIUS Authentication— uses RADIUS authentication for serial console access. • TACACS Authentication— uses TACACS + authentication, authorization, and accounting (AAA) services authentication for console access.
Read-Only Stack Password	Specifies the read-only password for stack or switch access.
Read-Write Stack Password	Specifies the read-write password for stack or switch access.

Configuring the Web and Telnet password using EDM

Use the following procedure to configure a password for Web and Telnet access to a stack, or standalone switch.

Related topics:

Procedure steps on page 30
Variable definitions on page 31

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Web/Telnet/Console**.

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

Variable definitions

Variable	Value
Web/Telnet Stack Password Type	Specifies the type of the password to use. Values include: • none—disables the password • Local Password— uses the locally defined password for Web and Telnet access. • RADIUS Authentication— uses RADIUS password authentication for Web and Telnet access. • TACACS Authentication— uses TACACS + authentication, authorization, and accounting (AAA) services authentication for Web and Telnet access.
Read-Only Stack Password	Specifies the read-only password for stack or switch access. The maximum length of the password is 15 characters.
Read-Write Switch Password	Specifies the read-write password for stack or switch access. The maximum length of the password is 15 characters.

Configuring ACLI banner

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

About this task

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

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

Procedure

1. Enter the Global Configuration mode in ACLI:
   ```
   enable
   configure terminal
   ```
2. Configure the switch to use a custom banner or use the default banner:
   ```
   banner {custom | static}
   ```
3. Create a custom banner:
   ```
   banner <line_number> "<LINE>"
   ```
4. Save the configuration:
   ```
   save config
   ```
5. Display the banner information:
   ```
   show banner
   ```
6. Logon again to verify the configuration.
7. **(Optional)** Disable the banner:
   ```
   no banner
   ```

Example

The following is an example of ACLI banner configuring:

```
4850GTS-PWR+>enable
4850GTS-PWR+#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4850GTS-PWR+(config)#show banner
Current banner setting: STATIC
4850GTS-PWR+(config)#banner custom
4850GTS-PWR+(config)#banner 1 "My Company Name"
4850GTS-PWR+(config)#banner 2 "123A My Address Avenue    My Town  CA 12345"
4850GTS-PWR+(config)#banner 3 "Phone: (123) 555-5555 * Fax (123) 555-5555"
4850GTS-PWR+(config)#banner 4 "http://www.mycompanywebsite.com"
```

```
4850GTS-PWR+(config)#save config
4850GTS-PWR+(config)#show banner
Current banner setting: CUSTOM
4850GTS-PWR+(config)#end
4850GTS-PWR+#exit
My Company Name
123A My Address Avenue    My Town  CA 12345
Phone: (123) 555-5555 * Fax (123) 555-5555
http://www.mycompanywebsite.com









Enter Ctrl-Y to begin.

  ************************************************************
  *** Ethernet Routing Switch 4850GTS-PWR+                 ***
  *** Avaya                                                 ***
  *** Copyright (c) 1996-2013,  All Rights Reserved         ***
  ***                                                       ***
  *** HW:R0B      FW:5.6.0.15  SW:v5.7.0.003                ***
  ************************************************************
```

Variable definition

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

Table 10: banner command

Variable	Value
custom	Disables the use of the default banner.
static	Activates the use of the default banner.
<*line_number*>	Banner line number you are setting. The range is 1–19
<LINE>	Specify the characters in the line number.

Configuring system identification

About this task

Configure system identification to specify the system name, contact person, and location of the switch. Also, to add trap receiver to the trap-receiver table.

Procedure

1. Enable Global Configuration mode in ACLI:
   ```
   enable

   configure terminal
   ```
2. Enable Simple Network Management Protocol (SNMP) server.
   ```
   snmp-server enable
   ```
3. Set the read-only community name.
   ```
   snmp-server community ro
   ```

   Note:

   Enter the community string two times.

   If you have run the install script to set up the configuration information, the read-only community name is already set.
4. Set the read-write community name.
   ```
   snmp-server community rw
   ```

   Note:

   Enter the community string two times.

   If you have run the install script to set up the configuration information, the read-write community name is already set.
5. Set the system name.
   ```
   snmp-server name "<text>"
   ```
6. Set the system contact.
   ```
   snmp-server contact "<text>"
   ```
7. Set the location.
   ```
   snmp-server location "<text>"
   ```
8. Configure SNMP host to add trap receiver to the trap-receiver table.
   ```
   snmp-server host <host-ip> <community-string>
   ```

Variable definitions

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

Table 11: snmp-server name command

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

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

Table 12: snmp-server contact command

Variable	Value
<*text*>	Specifies the SNMP system contact value. Enter an ASCII string of up to 255 characters.

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

Table 13: snmp-server location command

Variable	Value
<*text*>	Specifies the SNMP system location value. Enter an alphanumeric string of up to 255 characters.

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

Table 14: snmp-server host command

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

Enabling logging

Use this procedure to enable the logging of system messages. For more information about logging, see *Avaya Ethernet Routing Switch 2500, 4000, and 5000 Series Logs Reference* (NN47216-600).

Procedure

1. Enter Global Configuration mode in ACLI:

   enable

   configure terminal

2. To enable system log, enter the following command at the command prompt:
   `logging remote level informational`

Configuring Simple Network Time Protocol

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

Refer to *Configuration — System Avaya Ethernet Routing Switch 4000 Series, NN47205-500* for more information on SNTP.

About this task

You can configure the Network Time Protocol (NTP) servers for SNTP.

Procedure

1. Enable Global Configuration mode in ACLI:
   `enable`

   `configure terminal`

2. Enter the following command to configure the SNTP primary address:
   `sntp server primary address [<A.B.C.D> | <primary_server_ipv6address>]`

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

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

Note:

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

4. Enter the following command to enable SNTP:
   `sntp enable`

Variable definitions

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

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

Configuring local time zone

About this task

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

Procedure

1. Enter Global Configuration Mode in ACLI:
   `enable`
   `configure terminal`
2. Enter the following command to enable SNTP:
   `sntp enable`
3. Configure the time zone by using the following command:
   `clock time-zone zone hours [minutes]`
4. Configure daylight savings using the following command:

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

5. Save the changed configuration.

Example

Setting time zone example

```
4850GTS-PWR+>enable

4850GTS-PWR+#configure terminal

4850GTS-PWR+(config)#clock time-zone PST -8
```

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

Setting daylight savings time example

```
4850GTS-PWR+(config)#clock summer-time BST date 28 Mar 2013 2:00 30
Aug 2013 15:00 +60
```

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

Variable definitions

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

Table 15: clock time-zone command

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

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

Table 16: clock summer-time zone command

Variable	Value
date	Indicates that daylight savings time you set to start and end on the specified days every year.
day	Day to start daylight savings time.
month	Month to start daylight savings time.
year	Year to start daylight savings time.
hh:mm	Hour and minute to start daylight savings time.
day	Day to end daylight savings time.
month	Month to end daylight savings time.
year	Year to end daylight savings time.
hh:mm	Hour and minute to end daylight savings time.
offset	Number of minutes to add during the summer time.
zone	The time zone acronym to be displayed when daylight savings time is in effect. If it is unspecified, it defaults to the time zone acronym set when the time zone was set.

Configuring clock

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

About this task

Use the `clock source` command to set the time source for the switch.

Procedure

1. Enable Global Configuration mode in ACLI:
   ```
   enable

   configure terminal
   ```
2. Set the clock source for the switch.
   ```
   clock source {ntp | sntp | sysUpTime }
   ```

Related topics:

Variable definitions on page 40

Variable definitions

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

Variable	Value
ntp	Configure NTP as time source
sntp	Configure SNTP as time source
sysUpTime	Configure System Up Time as time source

Configuring static route

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

Procedure

1. Enter the Global Configuration command mode:
   ```
   enable

   configure terminal
   ```
2. Enable IP routing globally.
   ```
   ip routing
   ```
3. Configure IP address on a VLAN.
   ```
   ip address <ip address> <mask> [<MAC-offset>]
   ```
4. Configure a static route.
   ```
   ip route <destination ip> <mask> <next-hop> {<cost> | disable
   | enable | weight <cost>}
   ```
5. Display all the static routes.
   ```
   show ip route static [<dest-ip>] [-s <subnet> <mask>]
   ```
6. Save the configuration.

Variable definition

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

Table 17: ip route command

Variable	Value
<*ipaddr*>	Specifies the IP address to attach to the VLAN.
<*mask*>	Specifies the subnet mask to attach to the VLAN
<*MAC-offset*>	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address. The valid range is 1-256. Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.
<*destination ip*>	Specifies the destination IP address for the route being added. 0.0.0.0 is considered the default route.
<*mask*>	Specifies the destination subnet mask for the route being added.
<*next-hop*>	Specifies the next hop IP address for the route being added.
<*cost*>	Specifies the weight, or cost, of the route being added. Range is 1-65535.
enable	Enables the specified static route.
disable	Disables the specified static route.
weight <*cost*>	Changes the weight, or cost, of an existing static route. Range is 1-65535.

Enabling remote access

Use the following procedure to enable and configure remote access to the management features of the Avaya Ethernet Routing Switch 4000.

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series* (NN47205-102) and *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* (NN47205-500).

About this task

You can enable remote access for Telnet, SSH (on SSH software images), SNMP and Web Page Access.

Procedure

1. Enter Global Configuration mode in ACLI:

   enable

   configure terminal

2. To enable Telnet remote access, enter the following command at the command prompt:

   telnet-access enable

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

   ssh

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

   snmp-server enable

5. To enable Web Page remote access, enter the following command at the command prompt:

   web-server enable

Example

The following is an example of enabling Telnet remote access:

```
4850GTS-PWR+>enable
4850GTS-PWR+#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4850GTS-PWR+(config)#telnet-access enable
4850GTS-PWR+(config)#
```

Using telnet to log on to the device

About this task

Use Telnet to log on to the device and remotely manage the switch.

Procedure

1. From a PC or terminal, start a Telnet session:
   `telnet <IPv4_address>`

   - where <IPv4_address> is the IP address of the switch. The ERS 4000 standalone units use the default IP address of 192.168.1.1 if the switch does not get its IP address from another source.

2. Enter the logon and password when prompted.

Enabling the web management interface

About this task

The web server needs to be enabled to access EDM. If you do not wish EDM to be accessible on the device, disable the web server. By default web server is enabled.

Procedure

1. Enter the Global Configuration command mode in ACLI:
   ```
   enable

   configure terminal
   ```
2. At the command prompt, enter the following command:
   ```
   web-server enable
   ```

Accessing the switch through the Web interface

You can use the EDM to configure and maintain your switch through a Web-based graphical user interface

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

For more information about configuring the Web server to respond to HTTPS only, or both HTTPS and Hypertext Transfer Protocol (HTTP) client browser requests, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Before you begin

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

For more information about the supported browsers, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series*, NN47205-102

About this task

Monitor the switch through a Web browser from anywhere on the network. By default, the Web interface uses a 15 minute time-out period. If no activity occurs for 15 minutes, the system logs off the switch Web interface, and you must reenter the password information.

To configure inactivity time-out, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Procedure

1. Start your Web browser.
2. Type the switch IP address as the URL in the Web address field.
   `http://<IP Address>`

   `https://<IP Address>`
3. Enter the user name.
4. Enter the password.
5. Click **Log On**.

Configuring a VLAN

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

For more information on configuring a VLAN, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501.

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal
2. To create a VLAN, enter the following command at the command prompt:

   vlan create <VID_list> [name <LINE>] type { port { voice-vlan | remote-span | [<1-8>] { voice-vlan | remote-span } } | protocol decEther2 | protocol-ipEther2 | protocol-ipv6Ether2 | protocol ipx802.2 | protocol-ipx802.3 | protocol-ipxEther2 | protocol ipxSnap | protocol-Netbios | protocol-RarpEther2 | protocol sna802.2 | protocol-snaEther2 | protocol-vinesEther2

```
| protocol-xnsEther2 | protocol-Userdef {ether <4096-65534> |
llc <1-65534> | snap <1-65534>} | voice-vlan | spbm-bvlan |
spbm-switchedUni [<1-8>] } | [voice-vlan]
```

Example

The following is an example of creating a range of port-based VLANs:

```
4850GTS-PWR+(config)#vlan create 100,107,109-113,115 type port
4850GTS-PWR+(config)#
```

The following is an example of creating a protocol-based VLAN:

```
4850GTS-PWR+(config)#vlan create 200 type protocol-decEther2
```

The following is an example of creating and naming a voice-VLAN:

```
4850GTS-PWR+(config)#vlan create 300 name my_vlan type port voice-vlan
```

The following is an example of renaming an existing VLAN:

```
4850GTS-PWR+(config)#vlan name 300 my_vlan2
```

The following is an example of creating a VLAN using a user-defined protocol and specifying the frame encapsulation header type:

```
4850GTS-PWR+(config)#vlan create 500 type protocol-userdef ether 6004
```

The following is an example of creating an SPBM-BVLAN:

```
4850GTS-PWR+(config)#vlan create 600 type spbm-bvlan
```

The following is an example of creating an RSPAN VLAN:

```
4850GTS-PWR+(config)#vlan create 700 type port remote-span
```

The following is an example of displaying a range of VLANs:

```
4850GTS-PWR+(config)#show vlan id  100,107,109-113,115,200,300,500,600,700
Id   Name                 Type     Protocol         PID     Active IVL/SVL Mgmt
---- -------------------- -------- ---------------- ------- ------ ------- ----
100  VLAN #100            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
107  VLAN #107            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
109  VLAN #109            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
110  VLAN #110            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
111  VLAN #111            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
112  VLAN #112            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
113  VLAN #113            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
115  VLAN #115            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
200  VLAN #200            Protocol Declat Ether2    0x6004  Yes    IVL     No
       Port Members: NONE
300  my_vlan2             Voice    None             0x0000  Yes    IVL     No
       Port Members: NONE
500  VLAN #500            Protocol Ether2 User-Def. 0x1774  Yes    IVL     No
       Port Members: NONE
```

```
600  VLAN #600            B-VLAN   None             0x0000  Yes    IVL     No
       Port Members: NONE
700  VLAN #700            Port     None             0x0000  Yes    IVL     No
       Port Members: NONE
Total VLANs: 13
```

Variable Definitions

Variable	Value
<VID_list>	Enter as an individual VLAN ID to create a single VLAN or enter as a range of VLAN IDs to create multiple VLANs simultaneously. A VLAN ID can range from 1 to 4094. **Note:** VLAN ID values 4001 through 4008 are reserved and cannot be used.
name <line>	Specifies a unique alphanumeric name for an individual VLAN. **Note:** Do not enter a value for this parameter when you are creating multiple VLANs simultaneously.
type	Enter the type of VLAN to create: • port - port-based • protocol - protocol-based (see following list)
remote-span	Specify as RSPAN VLAN.
protocol-decEther2	Specify a decEther2 protocol-based VLAN.
protocol-ipEther2	Specify an ipEther2 protocol-based VLAN.
protocol-ipv6Ether2	Specify an ipv6Ether2 protocol-based VLAN.
protocol-ipx802.2	Specify an ipx802.2 protocol-based VLAN.
protocol-ipx802.3	Specify an ipx802.3 protocol-based VLAN.
protocol-ipxEther2	Specify an ipxEther2 protocol-based VLAN.
protocol-ipxSnap	Specify an ipxSnap protocol-based VLAN.
protocol-Netbios	Specify a NetBIOS protocol-based VLAN.
protocol-RarpEther2	Specify a RarpEther2 protocol-based VLAN.
protocol-sna802.2	Specify an sna802.2 protocol-based VLAN.
protocol-snaEther2	Specify an snaEther2 protocol-based VLAN.

Variable	Value
protocol-Userdef	Specify a user-defined protocol-based VLAN. Enter • *<4094 – 65534 >* {*<1-8>* | voice-vlan} - Ethernet II Userdef VLAN with this Protocol ID, where <1-8> is Spanning Tree Group ID • ether *<4096 – 65534>* –Ethernet II Userdef VLAN with this Protocol ID • llc *<1-65534>* –LLC Userdef VLAN with this Protocol ID • snap *<1-65534>* – SNAP Userdef VLAN with this Protocol ID
protocol-xnsEther2	Specify an xnsEther2 protocol-based VLAN.
protocol-vinesEther2	Specify a vinesEther2 protocol-based VLAN.
<1-8>	Specifies the Spanning Tree Group ID.
spbm-bvlan	Specify as SPBM B-VLAN.
spbm-switchedUni	Specify as SPBM switched UNI.
voice-vlan	Specify as Voice VLAN.

Configuring VLAN using EDM

Create a VLAN by IP subnet, port, protocol, or source MAC address using EDM.

Assign an IP address to the VLAN. You can also assign a MAC-offset value that allows you to manually change the default MAC address.

Before you begin

Ensure you follow the VLAN configuration rules for Ethernet Routing Switch 4000. For more information on the VLAN configuration rules and on configuring a VLAN, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501.

About this task

Create a VLAN and assign an IP address to a VLAN to enable routing on the VLAN.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.

3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** box, type the VLAN name, or use the name provided.
6. In the **StgId** specify the IDs to associate STG with the selected VLAN or VLANs.
7. In the **Type** box, select the type of VLAN you want to create.
   - To create a VLAN by port, choose **byPort**.
   - To create a VLAN by protocol, choose **byProtocolId**. This activates additional fields to configure protocol-based VLANs, including a selection of various protocols.
   - To associate SPBM network instance with one backbone VLAN in the core SPBM network, choose **spbm-bvlan**.
   - To use VLAN and create an endpoint to one I-SID and another port to create an endpoint to another I-SID, choose **spbm-switchedUni**.
8. Select **VoiceEnabled** to indicate whether a VLAN is voice VLAN.
9. Select **RspanEnabled** to indicate whether a VLAN is RSPAN enabled.

Variable definitions

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

Table 18: VLAN using EDM

Variable	Value
Id	Specifies the ID for the VLAN.
Name	Specifies an alphanumeric name for the VLAN. If you do not type a name, the switch default is applied.
StgId	Specifies the Spanning Tree Group (STG) to associate with the selected VLAN or VLANs. This is a read-only value. **Important:** This column is available only when the Spanning Tree administration operating mode is avayaSTG mode, when the operating mode is Multiple Spanning Tree Protocol (MSTP) or Rapid Spanning Tree

Variable	Value
	Protocol (RSTP), this column is not available.
Type	Indicates the type of VLAN. This is a read-only value. Values include: • byPort—VLAN by Port • byProtocolId—VLAN by Protocol ID • spbm-bvlan—backbone VLAN for the Shortest Path Bridging MAC (SPBM) • spbm-switchedUni—to create one endpoint on one Service Instance Identifier (I-SID) and another endpoint on another I-SID.
VoiceEnabled	Indicates whether VLAN is a voice VLAN (true) or not (false).
RspanEnabled	Indicates whether VLAN is an RSPAN VLAN (true) or not (false).
ProtocolId	Indicates the protocol identifier for the VLAN. The protocol ID is significant only when the VLAN type is byProtocolId. Values include: • ip • ipx802dot3 • ipx802dot2 • ipxSnap • ipxEthernet2 • decLat • sna802dot2 • snaEthernet2 • netBios • xns • vines • ipv6 • usrDefined • rarp

Installing a license file

This procedure is used to install a license file. If the switch is reset to default, the license file must be reinstalled and 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 Avaya Ethernet Routing Switch 4000 to enable licensed features.

Procedure

1. Log on to Privileged EXEC mode in ACLI:
   `enable`
2. Install a license file:
   `copy [tftp | usb] license <tftp_ip_address> filename <license_file_name>`
3. Restart the switch.

Example

Installing a license using USB example

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:

   ```
   4850GTS-PWR+>enable

   4850GTS-PWR+#copy usb license 4500_adv.lic
   ```

   The switch generates the message: `License successfully downloaded`

Important:

You must reboot the system to activate the license.

Saving the configuration

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

Before you begin

- You must log on to Privileged EXEC mode in ACLI.
- Enable the Trivial File Transfer Protocol (TFTP) on the switch.

About this task

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

Procedure

Save the running configuration:

```
save config
```

Storing the configuration files

Before you begin

- If you use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), ensure that you enabled the FTP or TFTP server. File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.
- You must log on to the Privileged EXEC mode in ACLI.

About this task

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

Avaya recommends that you keep several copies of backup files.

Procedure

At the command prompt, enter the following command:
`copy config usb {filename <filename> | unit <1-8>`

Variable definitions

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

Table 19: copy config usb command

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

Shutting down and resetting a switch

Shutting down the switch

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

Important:

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

Procedure

1. Log on to Privileged EXEC mode in ACLI:
   `enable`
2. Enter the following command:

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

Variable definition

Use the data in the following table to use the .

Table 20: shutdown command

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

Reloading remote devices

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

This procedure does temporarily disable auto-save functionality until the reload occurs. Cancelling the reload returns auto-save functionality to any previous setting.

About this task

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

Caution:

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

Procedure

1. Log on to Privileged EXEC mode in ACLI:
   enable
2. Enter the following command:

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

Variable definition

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

Table 21: reload command

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

Chapter 6: Verification

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

Pinging an IP device

About this task

Ping a device to test the connection between Avaya Ethernet Routing Switch 4000 and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, then it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, then the message indicates the address does not respond.

Procedure

1. Enter the User EXEC command mode in ACLI.
2. To ping an IP network connection, enter the following command:
   ping <IP_address>
   - where <IP_address> is an IPv4 or IPv6 address.

Verifying the software release

About this task

Displays the currently loaded and operational software load

Procedure

1. Enter the User EXEC command mode in ACLI.
2. Enter the following command to verify the software load.
   `show boot [diag] [image]`

Variable definitions

The following table describes the optional parameters you can enter with the **show boot [diag] [image]** command.

Variable	Value
diag	Displays only information for the agent load.
image	Displays only information for the image load.

Important:

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

Displaying local alarms

View local alarms to monitor alarm conditions.

About this task

Local alarms are raised and cleared by applications running on the switch. Local alarms are an automatic mechanism run by the system that do not require any additional user configuration. The raising and clearing of local alarms also creates a log entry for each event. Check alarms occasionally to ensure no alarms require additional operator attention.

Procedure

1. Enter Global Configuration Mode:

   ```
   enable
   configure terminal
   ```

2. To display local alarms, enter the following command at the command prompt:

   ```
   show rmon alarm
   ```

Chapter 7: Next steps

For more information about documents on how to configure other Avaya Ethernet Routing Switch 4000 features, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

For more information on new features of the Ethernet Routing Switch 4000 and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 4000 Series*, NN47205-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

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