User Interface Fundamentals
Avaya Ethernet Routing Switch 8800/8600

Release 7.2.10
NN46205-308
Issue 07.01
July 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose of this document

This document describes how to navigate the Command Line Interface (CLI), the Avaya Command Line Interface (ACLI), and the Enterprise Device Manager (EDM). It also describes the Configuration and Orchestration Manager.

Related resources

Documentation

See the *Avaya Ethernet Routing Switch 8800/8600 Documentation Roadmap*, NN46205-103, for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the website at http://avaya-learning.com/.

Avaya Mentor videos

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

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

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

Support

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

Chapter 2: New in this release

There are no new features to *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals,* (NN46205-308) for Release 7.2.10.

Other changes

This section lists the non-feature changes to this document for Release 7.2.10.

Web server

Changed the Web server default setting to disable.

Chapter 3: Fundamentals

The CLI, ACLI, and EDM are single-element configuration managers. You can use any one of these managers to configure your Avaya Ethernet Routing Switch 8800/8600. Which one you choose is strictly a personal preference. However, here are some characteristics to help you decide:

- CLI—This interface is an industry-standard command line interface. You may want to choose the CLI if you are used to configuring devices from other companies.
- ACLI—This interface is Avaya's traditional command line interface. You may want to choose the ACLI if you are used to configuring Avaya devices.
- EDM—This is a graphical user interface as opposed to a command line interface. Another distinction of EDM is that you can create graphical representations of statistics, which you cannot do with the command line interfaces.

The Configuration and Orchestration Manager (COM) is also a GUI like EDM, but it is installed on a remote server and it enables you to configure multiple devices through one interface

The following sections describe each of the interfaces in more detail:

CLI

You configure and manage the Ethernet Routing Switch with the Command Line Interface (CLI). The CLI is organized into a tree data structure. After you type a command, the prompt shows the command context (the current level or branch) and the command subcontext. Context indicates commands at the current level, and subcontext shows a list of commands available at that level. The following example shows the screen output, including context and subcontext, for the **config vlan 1 info** command.

```
ERS-8610:6/config/vlan/1# info
Sub-Context: create fdb-entry fdb-filter fdb-static ip ipv6 ipx ports srcmac static-
mcastmac
```

While you are at a level of the hierarchy, you need to type only the subcommand for that level. For example, to view the configuration information of VLAN 1 from the top or prompt level, type **config vlan 1 info**. If you are already at the **config vlan** branch, you need to type only **info**. In addition, while you are at a certain level, you remain at that level until you type **box** or **top**. These two commands return the CLI context to the system-level prompt. You use

the command context to create, delete, or change all relevant parameters for a port without reentering information.

ACLI

ACLI is an industry standard CLI that you can use for device management across Avaya products.

The ACLI has five major command modes, listed in order of increasing privileges. After you start a session on the switch, you begin in user EXEC mode. entering **`enable`** followed by a login name and password enters you into the privileged Exec mode. From privileged Exec mode, you can type any EXEC command or go to global configuration mode. From global configuration mode, you can enter either the interface configuration mode or the router configuration mode, depending on whether you want to configure an interface or a protocol.

Each mode provides a specific set of commands. The command set of a privilege mode at a higher level is a superset of a privilege mode at a lower level. You can access all privilege mode commands below a privilege mode at a higher level.

The command modes are:

- user EXEC—the initial mode of access. Only a limited number of commands are available in EXEC mode.
- privilege EXEC—accessed from the user EXEC mode. After you access this mode, you are prompted to provide a login name and password. The login name and password combination determines your access level in the privileged Exec mode and higher modes. Type **`enable`** to enter this mode from user EXEC mode. At the password prompt, type **`avaya`**. Most EXEC commands are one-time commands, such as show commands, which show the current configuration status. The EXEC commands are not saved across reboots.
- global configuration—use this mode to make changes to the running configuration. If you save the configuration, these settings survive a reboot of the switch.
- interface configuration—use this mode to modify either a logical interface, such as a virtual local area network (VLAN), or a physical interface, such as a port/slot. You can configure the following interfaces:
  - FastEthernet
  - GigabitEthernet
  - Loopback
  - MLT
  - VLAN
- router configuration—use this mode to modify a protocol. The protocols you can configure are:
  - BGP

- OSPF
- RIP
- VRRP
- VRF

From either the global configuration mode or the Interface configuration mode, save all of the configuration parameters (both global and interface) to a file. The default name for the configuration parameter file is config.cfg. You can also use alternative file names.

The following table lists the ACLI command modes, the prompts for each mode, the abbreviated name for each mode, and how to enter and exit each mode.

Table 1: ACLI command modes

Command mode	Prompt	Mode name	Command mode or enter/ exit mode
User EXEC	ERS-8600:5>	exec	This mode is the default command mode and does not require an entrance command. To exit the ACLI, enter **logout**.
privileged Exec	ERS-8600:5#	privExec	Enter **enable** to enter privileged Exec mode from user EXEC mode. Enter **disable** to exit privileged Exec mode and enter User EXEC mode. To exit the ACLI, enter **logout**.
Global configuration	ERS-8600:5<config>#	config	Enter **configure** to enter Global configuration mode from privileged Exec mode. Enter **exit** to exit Global configuration mode and enter privileged Exec mode. To exit the ACLI, enter **logout**.
Interface configuration	ERS-8600:5<config-if>#	config-if	Entry into this command mode depends on the type of configured interface. Enter **interface** {atm|FastEternet| GigabitEthernet| Loopback|mlt|pos| VLAN} to enter Interface configuration mode from Global configuration mode.

Command mode	Prompt	Mode name	Command mode or enter/ exit mode
			Enter **exit** to exit Interface configuration mode and enter Global configuration mode. To return to privileged Exec mode, enter **end**. To exit the ACLI, enter **logout**.
Router configuration	ERS-8600:5<config-router>#	config-router	Entry into this command mode is dependent on the configured protocol. Enter **router** {bgp|ospf|rip|vrrp|vrf} to enter Router configuration mode from Global configuration mode. Enter **exit** to exit Router configuration mode and enter Global configuration mode. To return to privileged Exec mode, enter **end**. To exit the ACLI, enter **logout**.

Enterprise Device Manager

Hypertext Transfer Protocol Secure (HTTPS) is the default method to connect to Enterprise Device Manager (EDM) over a Web browser. If you require a non-secure connection (HTTP) you can use CLI or ACLI to disable the Web server secure-only option. You cannot use EDM to configure HTTPS or HTTP access.

Secure access to EDM using HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is the default Web access method to connect to your switch with Enterprise Device Manager (EDM). If you need to use non-secure connections to EDM, for example HTTP, you must disable the Web server secure-only option.

Note:

You can connect through HTTP to an Ethernet Routing Switch 8800/8600 interface that has an IPv4 address, but not to an interface that has an IPv6 address.

HTTPS is the use of Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS).

Your HTTP browser, the HTTP client, acts as a TLS client and connects to the HTTP server, which acts as a TLS server.

When you start an SSL session for the first time your browser sends a request to the Web server. If you place an HTTPS prefix in the URL, the request places port number 443 into the packets. By deafult, port 443 is the number assigned to the SSL application on the server.

After your browser and the Web server acknowledge each other, the browser sends the server a list of algorithms it supports.

The server responds with an algorithm selected from the list and a signed digital certificate.

Note:

The server supports anonymous authentication and does not support client authentication. Client certificates are neither requested nor used by the server.

Your browser accepts and installs the server certificate and uses the certificate for all future connections.

From an internal list of certificate authorities (CAs) and their public keys, your browser validates the signed certificate from the server with the appropriate public key.

Both sides, your browser and the Web server, also send each other random numbers.

Your browser extracts the Web site public key from the server certificate. Then your browser uses the public key to encrypt a pre-master key which it sends to the server.

At each end, the client and server independently use the pre-master key and random numbers passed earlier to generate the secret keys that they use to encrypt and decrypt the remainder of the session.

The following figure illustrates the interaction between your browser and the HTTPS server when you connect using HTTPS.

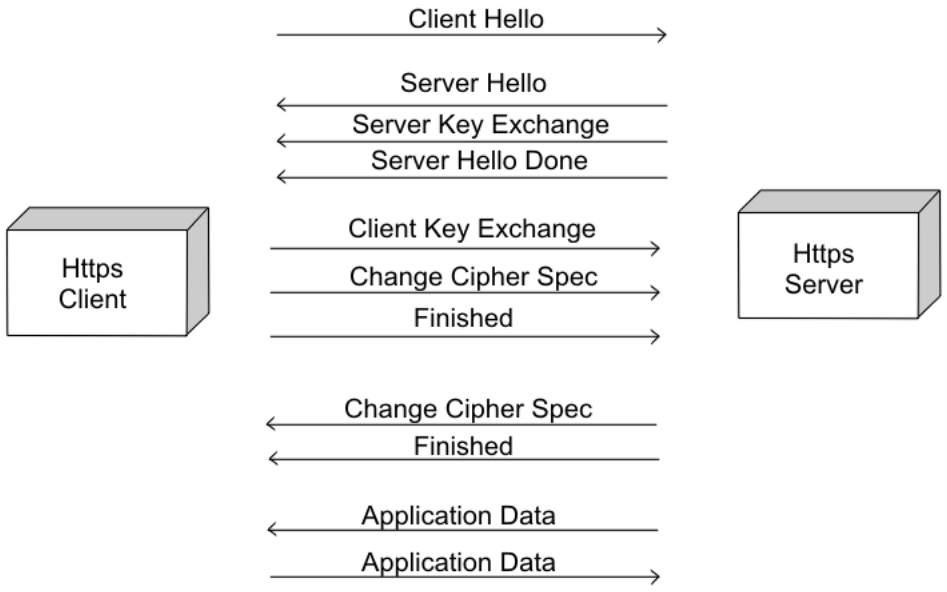


Figure 1: HTTPS access events

You can configure the Web server function for your switch, using either CLI or ACLI.

The Web server default option, secure-only enabled, provides a maximum of 5 HTTPS sessions and no HTTP sessions.

If you disable the secure-only option, a maximum of 5 sessions are available for any combination of HTTPS and HTTP.

The switch supports all current cipher suites supported by Open SSL version 0.9.5 as follows:

- 3DES
- Blowfish
- DH
- MD5
- RC4

Supported browsers

For EDM to display and function correctly, use one of the following Web browsers:

- Mozilla Firefox, versions 8.x and 9.x
- Microsoft Internet Explorer, versions 8.x and 9.x

Important:

You cannot open two HTTP sessions from the same IP address to the same switch using the same browser. To open two simultaneous sessions to the same switch, you must open one session in Internet Explorer and another in Firefox.

Default EDM username and password

For EDM access, the default username and password combination is admin/password.

Important:

If you have configured a username and password for Web server access in a previous release, these configured values remain unchanged. To access EDM, use these previously configured username and password values. In this case, the default values do not apply.

EDM help file

While the EDM GUI is bundled with the Ethernet Routing Switch 8800/8600 software, the associated EDM help files are not. To access the help files from the EDM GUI, you must install the EDM help files on a TFTP or FTP server in your network. For more information, see Installing EDM help files on page 56.

Device view

When you access EDM, the first screen displays a real-time physical view of the front panel of a device as shown in the following figure. From the front panel view, you can view configuration, and performance information for the device, a module, or a single port. This view is always available to you by clicking on the **Device Physical View** tab above the device view.

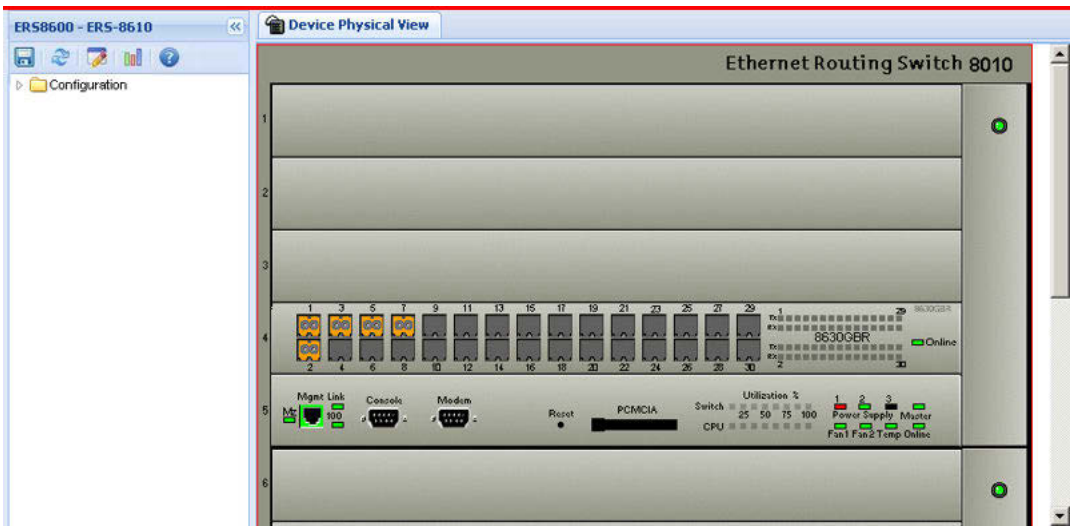


Figure 2: Device Physical View

You can use the device view to determine at a glance the operating status of the various modules and ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects. In the device view, you can select a module, port, power supply, or the entire chassis. To select an object, click the object. The object is outlined in yellow, indicating that it is selected.

The conventions on the device view are similar to the actual switch appearance. The module LEDs and the ports are color-coded to provide at-a-glance status. Green indicates the module or port is up and running; red indicates it is disabled.

Port color codes

The ports in the Physical Device View are color-coded to provide at-a-glance port status. The following table shows the status assigned to each color.

Table 2: Enterprise Device Manager port color codes

Color	Description
Green	Port is up and operating.
Red	Port is manually disabled.
Orange	Port has no link.
Light Blue	Port is in standby mode.
Dark Blue	Port is being tested.
Grey	Port is not reachable by Device Manager.
Pink	Port has a loopback connector connected to it.

EDM window

When you are working in EDM, you see a display similar to what is shown in Figure 3: Parts of the EDM window on page 19. This figure shows the following four parts of the EDM window:

- navigation tree—This is in the navigation pane on the left side of the window that displays all the available command tabs in a tree format. A row of buttons at the top of the navigation tree provides a quick method to perform common functions.
- menu bar—This area at the top of the window shows the most recently accessed primary tabs and their respective secondary tabs. When you select a primary tab, its secondary tabs are shown in the second layer. A primary tab can be docked or undocked, and the default is docked.
- toolbar—This area just below the menu bar gives you quick access to the most common operational commands such as **Insert**, **Delete**, **Apply**, **Refresh**, and **Help**.
- work area—The main area on the right side of the window displays the dialog boxes where you view or configure parameters on the switch.

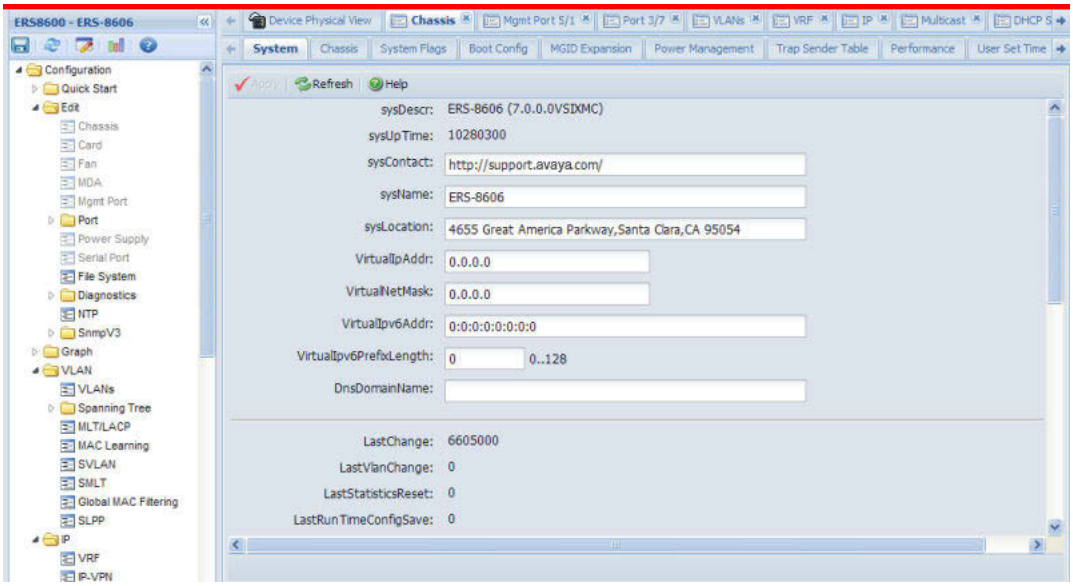


Figure 3: Parts of the EDM window

Navigation tree

You can use the navigation tree to see what commands are available and to quickly browse through the command hierarchy. A row of buttons at the top of the navigation tree provides a quick method to perform common functions.

Important:

Menu options related to a specific module are activated only after the chassis contains the required module, and you must select that module.

The following table describes the buttons that appear at the top of the navigation tree.

Table 3: Navigation pane buttons

Button	Name	Description
	Save Config	Saves the running configuration.
	Refresh Status	Refreshes the Device Physical View.
	Edit	Edits the selected item in the Device Physical View.
	Graph	Opens the graph options for the selected item in the Device Physical View.
	Help Setup Guide	Opens instructions about how to install the Help files and configure EDM to use the Help files.

Expand a folder by clicking it. Some folders have subfolders such as the Edit folder, which has the Port, Diagnostics, and SNMPv3 subfolders.

Within each folder and subfolder, there are numerous tabs. To open a tab, click it. The selected tab appears in the menu bar and opens in the work area. The following table describes the main folders in the navigation tree.

Table 4: Navigation tree folders

Menu	Description
Device	Use the Device menu to refresh and update device information or enable polling or hot swap detection. • Preference Setting — Enable polling or hot swap detection. Configure the frequency to poll the device. • Refresh Status — Use this option to refresh the device view. • Rediscover Device — Use this to trigger a rediscovery to update all of the device information.

Menu	Description
VRF Context view	Use the VRF Context view to switch to another VRF context view when you use the embedded EDM. GlobalRouter is the default view at log in. You can configure both Global Router (GRT) and Virtual Routing and Forwarding (VRF) instances when you launch a VRF context view. You can open only five tabs for each EDM session.
Edit	Use the Edit menu to view and configure parameters for the chassis or for the currently selected object. The selected object can be a module, fan, port, power supply, or another object. You can also use the Edit menu to perform the following tasks: • check and update security settings for the device • run diagnostic tests • change the configuration of the file system, NTP, service delivery, and SNMPv3 settings for the device
Graph	Use the Graph menu to view and configure EDM statistics and to produce graphs of the chassis or port statistics.
VLAN	Use the VLAN menu to view and configure VLANs, spanning tree groups (STG), MultiLink Trunks/LACP, MAC Learning, SMLT, Global MAC Filtering, and SLPP.
IP	Use the IP menu to view and configure IP routing functions for the system, including TCP/UDP, OSPF, RIP, VRRP, Multicast, IGMP, DHCP, BGP, RSMLT, PIM, UDP forwarding, and policies.
IPv6	Use the IPv6 menu to view and configure IPv6 routing functions, including TCP/UDP, tunnels, and OSPF.
Security	Use the Security menu to view and configure policies, filters, and protocols such as RADIUS, SSH, and EAPOL.
QOS	Use the QOS menu to view and configure QoS mapping tables, filters, profiles, and policy statistics.
Serviceability	Use the Serviceability menu to view and configure RMON alarms and view the RMON

Menu	Description
	alarm log and history log. You can use this menu to enable or disable RMON history or statistics on all ports. You can also use the Serviceability menu to view and configure IP Flow Information eXport (IPFIX).
Applications	Use the Applications menu to view and configure VSPTalk.

Menu bar

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

- The top row displays the tabs that you accessed through the navigation tree. These tabs are called primary tabs and they appear in the sequence that you accessed them.
- When you click on a primary tab, the secondary tabs associated with it appear in the bottom row. Click on any of the secondary tabs to display its dialog box.

In both the top and bottom rows of the menu bar, arrows appear on the left and right sides when the number of tabs exceeds the available space. Click on either arrow to scroll to the tab that you want to select.

To reduce the number of tabs on the top row, you can click on the X on the top right of a tab to remove it from the row. The following figure shows a sample menu bar.

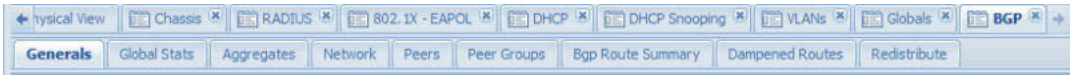


Figure 4: Menu bar

Toolbar

The toolbar buttons provide quick access to commonly used operational commands. The buttons that appear vary depending on the selected tab. However, the **Apply**, **Refresh**, and **Help** buttons are on almost every screen. Other common buttons are **Insert** and **Delete** and all table widgets in EDM have buttons for **Copy**, **Paste**, **Undo**, and **Print**.

- **Apply**—Use this button to execute any edits that you make.
- **Refresh**—Use this button to refresh any data on the screen.
- **Help**—Use this button to display online help that is context sensitive to the current dialog box.
- **Insert**—Use this button to display a secondary dialog box related to the selected tab. After you edit the configurable parameters, click the **Insert** button on the dialog box. This causes a new entry to appear on the dialog box of the selected tab.
- **Delete**—Use this button to delete a selected entry.

- **Copy**—Use this button to copy the information from a selected entry.
- **Paste**—Use this button to paste copied information into a new cell.
- **Undo**—Use this button to rollback any unsaved values on the table.
- **Print**—Use this button to print the current table.

The following figure shows a sample toolbar.

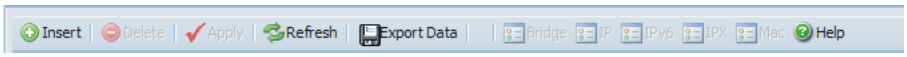


Figure 5: Toolbar

Work area

The work area is the main area on the right side of the window that displays the configuration dialog boxes. This is where you view or configure parameters on the switch.

The following figure is a sample work area showing the dialog box for the **Chassis** > **System** tab. If you want to compare the information in two dialog boxes, you can undock one and open another tab. For more information on this EDM feature, see Undocking and docking tabs on page 60.

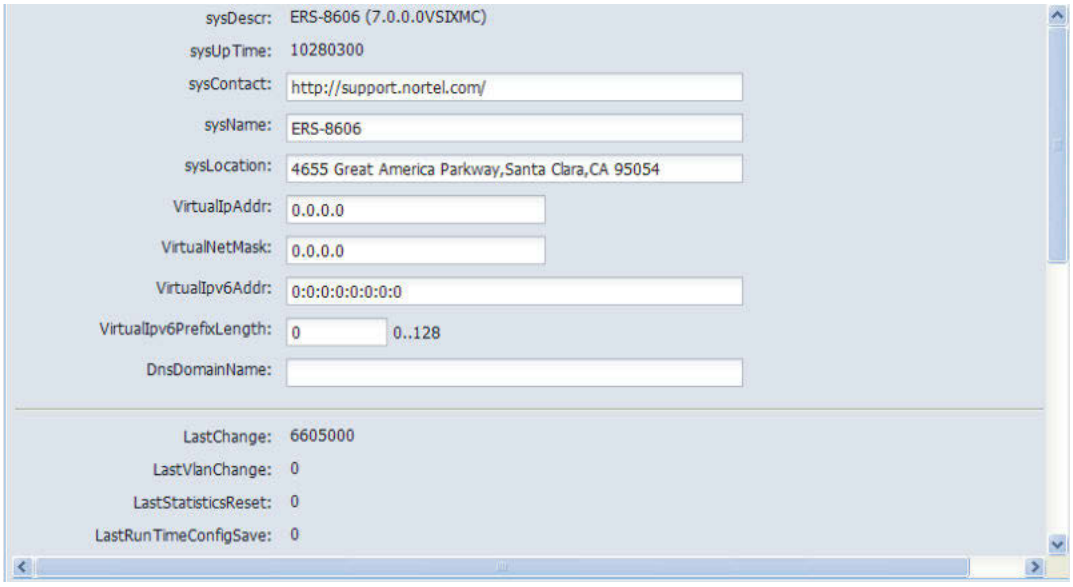


Figure 6: Work area

Column Sorting

When you click on the column heading in any table, all records in that table will be sorted in ascending or descending order, according to your selection, and the first 100 results will be shown on the first page. You can switch between pages of values by clicking on the **Next** or **Back** buttons at the bottom of the current page. Column sorting is based on the table field data

in the selected column. For example, if you click on the **Interface** column heading, the data will be sorted according to the interface index value, rather than the interface name.

Idle Timeout

If you allow your EDM session to remain idle for 10 minutes, EDM will offer a warning and a chance to extend the session. If you choose to extend the session, then EDM will remain logged in for another 15 minutes. Otherwise, the session will automatically expire after 5 minutes.

Preference Settings for Status Polling and Hot Swap Detection

In previous releases, you had to manually refresh to get updated LED and Port Status. Beginning with release 7.1.3, you can specify the polling interval for when the switch updates the LED and Port status. You can also set a preference to check for hot swaps and for how often you want to get updated information in the Physical View. When Hot Swap Detection is enabled, EDM will show a visual indicator to let you know if a module has been physically removed from or inserted into the switch.

For information on how to configure Status Polling, see Configuring Status Polling on page 69.

For information on how to configure Hot Swap Detection, see Configuring Hot Swap Detection on page 70.

Configuration and Orchestration Manager

Configuration and Orchestration Manager (COM) is an Avaya management system that allows you to manage multiple network devices. COM provides an interface to configure, manage, and provision Avaya enterprise devices, including Avaya Ethernet Routing Switch 8800/8600 switches, operating within the same local area network.

For more information about COM, see *Avaya Configuration and Orchestration Manager – Using the Product Interfaces (NN47226-100)*.

Chapter 4: HTTPS configuration procedures

Use the procedures in this section to configure and manage access to EDM over a Web browser.

Configuring HTTP mode

If you do not require secure connection to the switch over the Web, use the following procedure to disable the Web server secure-only option. Both HTTP and HTTPS connections are available. You can use CLI or ACLI to disable the secure-only option.

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt, enter the following command:

   ```
   config web-server secure-only disable
   ```

3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

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

Configuring HTTPS mode

If you disable HTTPS mode and require secure connection to the switch over the Web, use the following procedure to re-enable the Web server secure-only option. Only HTTPS connections will be available. You can use CLI or ACLI to enable the secure-only option.

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt enter the following command:

```
config web-server secure-only enable
```

3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

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

Configuring HTTP port number

Use this procedure to allocate a port, other than the default, for HTTP use.

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt enter the following command:

   ```
   config web-server http-port <1-49151>
   ```

   The default is port 80.
3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

   ```
   web-server http-port <1-49151>
   ```

   The default is port 80.

Configuring HTTPS port number

Use this procedure to allocate a port, other than the default, for HTTPS use.

Important:

Avaya strongly recommends that you discover the ports that UDP and TCP are already using before you select a port for HTTPS. Use the following commands to list the ports already in use and then select a port that is not in the resulting list.

For the CLI, use: **`show ip tcp info-connections`** and **`show ip udp endpoints.`**

For the ACLI, use: **`show ip tcp connections.`**

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt enter the following command:

   ```
   config web-server https-port <443 | 1024-49151>
   ```

   The default is port 443.
3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

   ```
   web-server https-port <443 | 1024-49151>
   ```

   The default is port 443.

Setting HTTP port number to default

Use this procedure to return the HTTP port to the default value.

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt enter the following command:

   ```
   config web-server http-port 80
   ```
3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

   ```
   default web-server http-port
   ```

Setting HTTPS port number to default

Use this procedure to return the HTTPS port to the default value.

Procedure steps

1. Open a telnet connection to the switch.
2. If you are using CLI, at the prompt enter the following command:

   ```
   config web-server https-port 443
   ```

3. If you are using ACLI, access the Global Configuration mode. At the prompt, enter the following command:

   ```
   default web-server https-port
   ```

Chapter 5: CLI procedures

This section contains information about common CLI tasks.

Exiting and entering the CLI

End a CLI session with the following procedure.

Procedure steps

1. End a CLI session with one of the following commands:
   - `quit`
   - `logout`
   - `exit`
2. Enter the following command to log back on to the CLI.

   `login`

Using Edit commands

Use Edit commands to modify CLI command text, and navigate within commands.

Procedure steps

1. Type `ESC` to enter the edit mode.
2. Use the commands listed in the following table to make the edits.
3. Press the `Return` key to move to the next line.

Job aid: Commands available in edit mode

The following table lists CLI edit commands.

Key combination	Description
:q	End the editing mode without saving the changes made to a file.
:w	Quit and save the file.
ZZ	Quit and save the file.
Movement and Search Commands	
^L	Redraw the screen.
^F	Display the next screen.
^B	Display the previous screen.
^D	Display the next 1/2 screen.
^U	Display the previous 1/2 screen.
<*n* >G	Go to the command number *n*.
G	Go to the last command line.
/<*s*>	Search forward in the file for the string *s*.
?<*s*>	Search backward in the file for the string *s*.
n	Repeat the last search.
N	Repeat the last search in the opposite direction.
< *n*>k	Get the *nth* previous line in the file.
< *n*>-	Same as *k*.
< *n*>j	Get the *nth* next line in the file.
< *n*>+	Same as *j*.
RETURN	Same as *j*.
< *n*>h	Move left *n* characters.
^H	Same as *h*.
< *n*>l	Move right *n* characters.
SPACE	Same as 1.
< *n*>w	Move *n* words forward.
< *n*>W	Move *n* blank-separated words forward.
< *n*>e	Move to the end of the *nth* next word.

Key combination	Description
< *n*>E	Move to the end of the *nth* next blank-separated word.
< *n*>b	Move back *n* words.
< *n*>B	Move back *n* blank-separated words.
f< *c*>	Find character *c*, searching forward.
F< *c*>	Find character *c*, searching backward.
^	Move the cursor to the first non blank character in line.
$	Go to the end of the line.
0	Go to the beginning of the line.
Insert commands (input is expected until you type ESC)	
a	Append.
A	Append at the end of the line.
c SPACE	Change character.
cl	Change character.
cw	Change word.
cc	Change entire line.
c$	Change everything from the cursor to the end of the line.
C	Same as c$.
S	Same as cc.
i	Insert.
I	Insert at the beginning of the line.
R	Type over characters.
o	Open a line after the current line.
O	Open a line preceding the current line.
Editing commands	
< *n*>r< *c*>	Replace the following *n* characters with *c*.
< *n*>x	Delete *n* characters starting at the cursor.
< *n*>X	Delete *n* characters to the left of the cursor.
d SPACE	Delete character.
dl	Delete character.

Important:

The default value for < *n*> is 1.

Job aid: special terminal characters

The following table lists the special terminal characters.

Key Combination	Command
^H	Backspace.
^D	Log off of the CLI.
^C	Cancel the line entry.
^P	View the previous history command.
^N	View the next history command.
^S	Suspend the output.
^Q	Resume the output.
^I	Complete the command.
^B	Move the cursor back one character.
^F	Move the cursor forward one character.
^A	Move the cursor to the beginning of the line.
^E	Move the cursor to the end of the line.
ESC B	Move the cursor back one word.
ESC F	Move the cursor forward one word.
DEL	Erase the character at the cursor.
^K	Erase all characters from the cursor to the end of the line.
^X	Erase all characters before the cursor to the beginning of the line.
^U	Erase or clear the entire line.
^W	Erase the word to the left of the cursor.
ESC D	Erase from the cursor to the end of the word.
^L	Redisplay the line.
^R	Redisplay the line.
^T	Transpose the character to the left of the cursor with the character at the cursor.
ESC L	Change the character at the cursor to lowercase.
ESC U	Change the character at the cursor to uppercase.
;	Terminate multiple commands.

Key Combination	Command
"..."	Preserve white space in strings.

Displaying a directory

Display a directory to see the contents of the flash and PCMCIA memory.

Procedure steps

Display the contents of the flash and PCMCIA memory using the following command:

```
directory [<dir>] [<-l>]
```

Variable definitions

Use the data in the following table to use the **`directory[<dir>] [<-l>]`** command.

Table 5: Variable definitions

Variable	Value
dir	Specifies either flash or PCMCIA in the form /flash or /pcmcia.
-l	Displays file details if you specify a path name.

After you invoke the **`directory`** command with no arguments, the contents of all flash devices appear. After you specify flash or PCMCIA **`directory`**, only the contents of that device appear.

After you use the **`dir`** command, the CLI displays all file names under the parent directory, rather than under the subdirectory.

Copying files

Copy a files to move information from one memory storage area or medium to another.

Procedure steps

Copy a file using the following command:

`copy <srcfile><dstfile>`

Variable definitions

Use the data in the following table to use the **`copy <srcfile> <dstfile>`** command.

Variable	Value
<dstfile>	The destination file in the format {a.b.c.d:|peer:|/pcmcia/xxx|/flash/xxx}*<file>* and *file* is the file name of the destination file.
<srcfile>	The source file in the format {a.b.c.d:|peer:|/pcmcia/|/flash/}*<file>* and *file* is the filename of the source file.

Copying the runtime image to flash memory from a remote TFTP server

Use the following procedure to copy a runtime image to flash memory from a remote trivial file transfer protocol (TFTP) server.

Procedure steps

Copy a runtime image to flash memory from a remote TFTP server using the following command:

`copy <ip_address>:<filename> <destination>`

Variable definitions

Use the data in the following table to use the **`copy <ip_address> <filename> <destination>`** command.

Variable	Value
<*destination*>	The name of the copied file in its new location.
<*ip_address*>:<*filename*>	The source argument that specifies the IP address of the remote TFTP server and the name of the file you want to copy.

Examples of copying the runtime image

1. Copy a runtime image from a TFTP server to a local flash using the following command:

   ```
   copy 192.168.249.10:p80a4100.img /flash/p80a4100.img
   ```

2. Copy a runtime image from the TFTP server to a local PCMCIA using the following command:

   ```
   copy 192.168.249.10:p80a4100.img /pcmcia/p80a4100.img
   ```

3. Copy a runtime image from CPU-Slot5 flash to CPU-Slot6 flash using the following command: The IP address for CPU-Slot5 is 127.0.0.5; the IP address for CPU-Slot5 is 127.0.0.6.

   ```
   copy /flash/p80a4100.img 127.0.0.6:/flash/p80a4100.img
   ```

4. Copy a runtime configuration file to a TFTP server using the following command:

   ```
   copy /flash/config.cfg 192.168.249.10:config.cfg
   ```

Saving the configuration to a file

Use the following procedure to save the running configuration to a file.

Procedure steps

Save the running configuration to a file using the following command:

`save` <*savetype*> [file <value>] [verbose] [standby <value>] [backup <value>]]

Variable definitions

Use the data in the following table to save the running configuration to a file.

Variable	Value
backup <value>	Saves the specified file name and identifies the file as a backup file.
file <value>	The file name.
mode <value>	CLI or ACLI
<savetype>	Specifies the type of file to save. The options are: • config • bootconfig • log • trace • clilog • snmplog
standby <value>	Saves the specified file name to the standby CPU.
verbose	Saves the default and current configuration. If you omit the [verbose]parameter, only the current configuration is saved.

Getting Help

When you navigate the boot monitor and run-time CLI, Online Help is available at all levels. From any level of the tree, you can access Help in one of the following four ways:

- Entering **`help <command>`** explains what the command does and gives its syntax.
- Entering **`help`** at the system prompt provides an explanation of the available help.
- Entering<*command*> *syntax* displays a list of commands and parameters available for that command.
- Entering a question mark (**`?`**) at the prompt results in a list of all commands in that command context and the subcontext of that command.

Modifying user access

EDM read-write community users can modify their usernames and passwords. You can adapt the following example to restrict these users from modifying their usernames and passwords.

This example show how to create a user, **avaya**, and restrict the user from modifying the user name corresponding to read write access (rwa) through EDM.

Procedure steps

1. Create a mib-view (strict) that excludes the management information base (MIB) object identifiers (OID) corresponding to the user names and passwords of the access levels as follows:
   a. `ERS-8610:5/config/snmp-v3/mib-view# create strict 1`
   b. `ERS-8610:5/config/snmp-v3/mib-view# strict 1.3.6.1.4.1.2272.1.19.1 type exclude`
2. Create a user (Avaya) as follows:.

   ```
   ERS-8610:5/config/snmp-v3/usm# create Avaya
   ```
3. Create an snmp-group corresponding to the user (group) as follows:.

   ```
   ERS-8610:5/config/snmp-v3/group-member# create avaya usm group
   ```
4. Set the SNMP access for that group. You set the write permissions to the user based on the mib-view strict that you created in step 1, as follows:
   a. `ERS-8610:5/config/snmp-v3# group-access create group "" usm noAuthNoPriv`
   b. `ERS-8610:5/config/snmp-v3# group-access view group "" usm noAuthNoPriv read root write strict notify root`
5. Repeat steps 1 to 4 for the different access level user names and passwords to which you want to restrict write access.

Job aid: Mapping of access level names and passwords to OIDs

The following table shows the mapping between the available access level names and passwords to their corresponding OIDs.

Table 6: Mapping of access level names and passwords to OIDs

Object-ID	Object-ID name
1.3.6.1.4.1.2272.1.19.1	RWAUserName
1.3.6.1.4.1.2272.1.19.2	RWAPassword
1.3.6.1.4.1.2272.1.19.3	RWUserName
1.3.6.1.4.1.2272.1.19.4	RWPassword

Object-ID	Object-ID name
1.3.6.1.4.1.2272.1.19.5	RWL3UserName
1.3.6.1.4.1.2272.1.19.6	RWL3Password
1.3.6.1.4.1.2272.1.19.7	RWL2UserName
1.3.6.1.4.1.2272.1.19.8	RWL2Password
1.3.6.1.4.1.2272.1.19.9	ROUserName
1.3.6.1.4.1.2272.1.19.10	ROPassword
1.3.6.1.4.1.2272.1.19.15	RWL1UserName
1.3.6.1.4.1.2272.1.19.16	RWL1Password

Chapter 6: ACLI procedures

Either the ACLI or the CLI is accessible at runtime. You cannot use both the CLI and ACLI commands in the same session. If a switch is operating in ACLI mode, it does not recognize a CLI configuration file and therefore cannot load it. Similarly, a switch operating in CLI mode does not recognize an ACLI configuration file and cannot load it.

You use a boot monitor flag to toggle between the existing CLI and ACLI. You must reboot the switch for the change to take effect (if configured from runtime). Also, to retain the configuration, you must save the running configuration in the new mode before you toggle the flag.

The CLI and ACLI config files must have unique file names when you save them. If the file names are not unique, the configuration file is overwritten in either CLI format or ACLI format, depending on the choice you made. When you boot dual SF/CPU switches, always boot the secondary SF/CPU before you boot the primary SF/CPU. Avaya recommends that you reset and hold the secondary SF/CPU at the monitor prompt, and then boot the primary SF/CPU. After the primary SF/CPU boots, boot the secondary SF/CPU from the monitor prompt.

Note:

When changing to ACLI mode, the message "`Some SNMP commands may not be saved`" is shown.

Accessing the ACLI

When you first power up the Ethernet Routing Switch 8800/8600, the default interface is the CLI. To switch from the CLI to the ACLI, you must change the ACLI boot flag and save the boot configuration file.

Procedure steps

Change the ACLI boot flag using the following command:

```
ERS-8610:5# config bootconfig flags acli true
```

Important:

You must reboot the switch for this change to take effect. After you reboot the switch, access the ACLI using Telnet, rlogin, or the local console port.

Logging on to the software and accessing global configuration mode

After you access the ACLI, you can do the following:

- Log on to the software using the default user name and password.
- Access global configuration mode.

Procedure steps

1. At the login prompt enter the default value.
2. At the password prompt, enter the default password.
3. To access privExec mode, at the prompt `ERS-8610:5`, enter `enable`.
4. To access global configuration mode, at the prompt, enter `configure terminal`.

Switching from the ACLI back to the CLI

The config.cfg file for the CLI and the config.cfg file for the ACLI are not compatible. If you decide to change the CLI mode to ACLI, or the reverse, you must use the config.cfg file for the selected mode.

Prerequisites

- You must be in global configuration mode to switch from the ACLI to the CLI.

Procedure steps

Switch from ACLI to CLI using the following commands:

a. `ERS-8610:5(config)#no boot config flags acli`
b. `ERS-8610:5(config)# exit`

Viewing configurations

You can view all of the configurations in one mode even if the switch is in a different mode.

Procedure steps

1. View CLI configurations using the following command:

   ```
   show running-config mode cli
   ```

2. View ACLI configurations using the following command:

   ```
   show config mode acli
   ```

Saving the running configuration

You can save the running configuration on the switch in ACLI format from CLI, or in CLI format from ACLI.

Procedure steps

1. Save the running configuration from CLI to ACLI using the following command:

   ```
   ERS-8610:5# save config file testacli.cfg mode acli
   ```

2. Save the running configuration from ACLI to CLI using the following command in global configuration mode:

   ```
   ERS-8600:5(config)# save config file testcli.cfg mode cli
   ```

Switching from CLI to ACLI for a single CPU from factory defaults

If the switch is in CLI mode, when you set the bootconfig flag to ACLI, the system automatically saves the boot.cfg and prompts for a reboot in ACLI mode. The reverse is also true.

Prerequisites

- You must be in global configuration mode to switch from the ACLI to the CLI.

Procedure steps

1. Set the factory defaults flag on the switch.
2. Enter the following command:

   ```
   config boot flags acli true
   ```

3. Boot the switch.

Switching from CLI to ACLI for a single CPU from the existing configuration

Use the following procedure to change a single CPU from CLI to ACLI from an existing configuration.

Procedure steps

1. Save the configuration in ACLI mode.

   The following is an example:

   ```
   save config file acli.cfg mode acli
   ```

   Tip:

   Remember to use a file name other than that used in the CLI, otherwise the system overwrites the CLI config file.

2. Set the default config to the configured file name.
3. Boot the switch.
4. After the switch boots, source the configuration file with the following command:

   ```
   source /flash/acli.cfg
   ```

Switching from ACLI to CLI for a single CPU from factory defaults

Use the following procedure to change a single CPU from ACLI to CLI from factory defaults.

Procedure steps

1. Enter global configuration mode.
2. Enter the following command:

   ```
   boot config flags factory
   ```
3. Enter the following command:

   ```
   no boot config flags acli
   ```

   The boot.cfg file is saved automatically.
4. Boot the switch.

Switching from ACLI to CLI for a single CPU from existing configuration

Use the following procedure to change a single CPU from ACLI to CLI from an existing configuration.

Procedure steps

1. Save the configurations in CLI mode. The following is an example:

   ```
   save config file cli.cfg mode cli
   ```
2. Enter global configuration mode.
3. Enter the following command:

   ```
   no boot config flags acli
   ```
4. Boot the switch.

Switching from CLI to ACLI for a dual CPU (non-HA) from factory defaults

The savetostandby flag is enabled after you upgrade a dual CPU, not in high availability mode (non-HA), from the CLI to ACLI and from the ACLI to CLI from both factory defaults and existing configurations.

Procedure steps

1. Set the factory defaults flag on the switch and save the boot configuration.
2. Boot the secondary SF/CPU in ACLI mode. The secondary SF/CPU starts in ACLI mode.
3. Boot the primary SF/CPU in ACLI mode.

   Both CPUs are now in ACLI mode.

Switching from CLI to ACLI for a dual CPU (non-HA) from existing configurations

Use the following procedure to change a dual CPU from CLI to ACLI from an existing configuration.

Procedure steps

1. Save the configurations in ACLI mode.

   The following is an example:

   ```
   save config file acli.cfg mode acli
   ```

2. Enter the following command:

   ```
   config boot flags acli true
   ```

3. Boot the secondary SF/CPU first and then boot the primary SF/CPU.

Switching from ACLI to CLI for a dual CPU (non-HA) from factory defaults

Use the following procedure to change a dual CPU from ACLI to CLI from factory defaults.

Procedure steps

1. Set the factory defaults flag on the switch and save the boot configuration.
2. Boot the secondary SF/CPU in CLI mode.

   The secondary SF/CPU comes up in CLI mode.
3. Boot the primary SF/CPU in CLI mode.

   Both CPUs are now in CLI mode.

Switching from ACLI to CLI for a dual CPU (non-HA) from existing configurations

Use the following procedure to change a dual CPU from ACLI to CLI from existing configurations.

Prerequisites

- You must be in global configuration mode to switch from the ACLI to the CLI.

Procedure steps

1. Save the configurations in CLI mode.

   The following is an example:

   ```
   save config file cli.cfg mode cli
   ```
2. Enter the following command:

```
no boot config flags acli
```

3. Boot the secondary SF/CPU first and then boot the primary SF/CPU.

Switching from CLI to ACLI for an HA-CPU from factory defaults

The HA flag and savetostandby flag are enabled after you upgrade an HA-CPU from the CLI to ACLI and from the ACLI to CLI from both factory defaults and existing configurations.

In HA-SETUP, you must boot both the primary SF/CPU and secondary SF/CPU; otherwise, one is in CLI mode and other is in ACLI mode. When you toggle from ACLI to CLI, table synchronization does not occur if one SF/CPU is in CLI mode and the other SF/CPU is in ACLI mode.

Procedure steps

1. Set factory defaults flag on the switch and save the boot configuration.
2. Boot the secondary SF/CPU in ACLI mode.

   The secondary SF/CPU comes up in ACLI mode.
3. Boot the primary SF/CPU in ACLI mode.

   Both the secondary SF/CPU and primary SF/CPU are now in ACLI mode.

Switching from CLI to ACLI for an HA-CPU from existing configurations

Use the following procedure to change an HA-CPU from CLI to ACLI from an existing configuration.

Procedure steps

1. Save the configurations in ACLI mode.

   The following is an example:

   ```
   save config file acli.cfg mode acli
   ```
2. Enter the following command:

```
config boot flags acli true
```

3. Boot the secondary SF/CPU first and then boot the primary SF/CPU.

Switching from ACLI to CLI for an HA-CPU from factory defaults

Use the following procedure to change an HA-CPU from ACLI to CLI from factory defaults.

Prerequisites

- You must be in global configuration mode to switch from the ACLI to the CLI.

Procedure steps

1. Set the factory defaults flag on the switch and save the boot configuration.
2. Boot the secondary SF/CPU in CLI mode.

   The secondary SF/CPU comes up in CLI mode.
3. Boot the primary SF/CPU in CLI mode.

   Both the secondary SF/CPU and primary SF/CPU are now in CLI mode.

Switching from ACLI to CLI for an HA-CPU from existing configurations

Use the following procedure to change an HA-CPU from ACLI to CLI from existing configurations.

Prerequisites

- You must be in global configuration mode to switch from the ACLI to the CLI.

Procedure steps

1. Save the configurations in CLI mode.

   The following is an example:

   ```
   save config file cli.cfg mode cli
   ```

2. Enter the following command:

   ```
   no boot config flags acli
   ```

3. Boot the secondary SF/CPU first and then boot the primary SF/CPU.

Chapter 7: Enterprise Device Manager procedures

This section contains procedures for starting and using Enterprise Device Manager (EDM). The software is built-in to the switch so there is no need to install any additional software. For information about general EDM concepts, see Enterprise Device Manager on page 14.

Enabling the Web server using the CLI

Disabled by default, you can enable or disable Web access using the **config web-server** command.

Use the following procedure to enable and manage the Web server using the CLI. After you enable the Web server, you can start EDM.

Procedure steps

Enable and manage the Web server using the following command:

```
config web-server enable
```

For more information, see the following Variable definitions table.

Variable definitions

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

Table 7: Variable definitions

Variable	Value
def-display-rows <integer>	Sets the number of rows displayed on each page. • *integer* is 10 to 100.
disable	Disables the Ethernet Routing Switch Web interface.
enable	Enables the Ethernet Routing Switch Web interface.

Variable	Value
html-source-dir help-tftp <file>	Specifies the file location and name for the Web server HTML Help file. • *file* specifies the path and file name of the HTML source.
http-port <integer>	Specifies the HTTP port of the Web server. • *integer* is a value from 1 to 49151.
info	Indicates whether Web access is enabled or disabled on the switch and displays the current Web user name and password setting.
password <rwa> <username> <passwd>	Sets passwords for access to the Web interface. • *username* is the user's log on name, up to 20 characters long. Note that regardless of the username you choose, the access level provided to the Web/EDM user is rwa. • *passwd* is the password associated with the log on name, up to 20 characters long.
secure-only <enable|disable>	Enable secure-only to restrict the Web access mode to HTTPS. This is the default setting. Disable to allow HTTP access to the switch.

Example of configuring the Web server using the CLI

This configuration example shows you how to enable the Web interface, specify the number of rows in the display, and display Web interface parameters.

Procedure steps

1. Enable the Web interface using the following command:

   ```
   config web-server enable
   ```

2. Specify the number of rows in the display using the following command:

   ```
   config web-server def-display rows 25
   ```

3. Display the web interface parameters using the following command:

   ```
   config web-server info
   ```

4. Display if Web access is enabled as well as password and access information using the following command:

   ```
   show web-server
   ```

5. Disable the secure-only parameter using the following command:

```
config web-server secure-only disable
```

```
Web Server Info :
Status            : on
Secure-only            : disabledRWA Username              : admin
RWA Password              : ********
Def-display-rows          : 30
Html help tftp source-dir :
HttpPort                  : 80
NumHits                   : 57
NumAccessChecks           : 7
NumAccessBlocks           : 2
NumRxErrors               : 49
NumTxErrors               : 0
NumSetRequest             : 0
```

Enabling the Web server using the ACLI

Disabled by default, you can use the following procedure to enable and manage the Web server using the ACLI. After you enable the Web server, you can start EDM.

Procedure steps

1. In Global Configuration mode, enable the Web server using the following command:

   ```
   web-server enable
   ```

2. Disable the web server with the following command:

   ```
   no web-server enable
   ```

3. In the privEXEC configuration mode, display the web-server status using the following command:

   ```
   show web-server
   ```

For more information, see the following Variable definitions table.

Variable definitions

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

Table 8: Variable definitions

Variable	Value
def-display-rows	Sets the number of rows displayed on each page, between 10 and 100.
enable	Enables the Ethernet Routing Switch Web interface.

Variable	Value
	To disable the web-server, use the following command: `no web-server [enable]`
help-tftp	Specifies the file location and name for the Web server HTML Help file in the following format: *<WORD/0-256> {a.b.c.d:| peer: | /pcmcia/ | /flash/ |} <file> <string length 0..256>*
http-port	Specifies the HTTP port of the Web server. The value is from 1 to 49151.
password	Sets user names and passwords for access to the Web interface in the following format: *{rwa}<WORD/1-20> <WORD/1-20>* Note that regardless of the user name you choose, the access level provided to the Web/EDM user is rwa.
secure-only <enable|disable>	Enable secure-only to restrict the Web access mode to HTTPS. This is the default setting. Use the `no web-server secure-only` command to disable the web-server secure-only option and allow HTTP access to the switch.

Example of configuring the Web interface using ACLI

This configuration example uses the **`web-server`** commands to enable the web interface and specify the number of rows in the display. The example also uses the **`show`** command to display web interface parameters.

Procedure steps

1. Enable the web interface using the following command in global configuration mode:

   ```
   web-server enable
   ```

2. Specify the number of rows in the display using the following command:

   ```
   web-server def-display-rows 25
   ```

3. Display the web interface parameters using the following command:

   ```
   show web-server
   ```

4. Disable the secure-only parameter using the following command:

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

```
Web Server Info :
Status: on
Secure-only:  disabledRWA Username:  admin
RWA Password: ********
Def-display-rows: 30
Html help tftp source-dir:
HttpPort: 80
```

```
NumHits: 57
NumAccessChecks: 7
NumAccessBlocks: 2
NumRxErrors: 49
NumTxErrors: 0
NumSetRequest: 0
```

Using HTTPS to access EDM on the switch

Use this procedure to access your switch over a secure Web connection to EDM.

Prerequisites

- Make sure that the Ethernet Routing Switch 8800/8600 is running and you are connected to it
- Note the IP address of the Ethernet Routing Switch 8800/8600
- Open one of the supported browsers
- Ensure that port 443 is enabled on your network
- Note that HTTPS is the default access method. If you do not want to use HTTPS, use CLI or ACLI to disable the web-server option secure-only.

Important:

If you have configured a username and password for Web server access in a previous release, these configured values remain unchanged. To access EDM, use these previously configured username and password values. In this case, the default values do not apply.

Procedure steps

1. Open a supported Web browser.
2. In the dialog box, enter the following:

   https://<ipaddress:port>

   example: https://47.17.10.154:80
3. On the initial login page, enter the following:
   - User Name – the configured user name; default value is `admin`.
   - Password – the configured password; default value is `password`.

Note:

If you enter an incorrect User Name or Password, the system generates the following error message: **Authentification Failed!.** The system also generates the following error message on the console: **Error: The VRF Name entered does not correspond to any VRF**.

Variable definitions

Table 9: Variable definitions

Variable	Value
Device	IP address or DNS of your switch
Port	The default value is port 443 for SSL connections.

Changing user name and password using EDM

Once you have enabled the Web server and configured either HTTPS or HTTP access, using either CLI or ACLI, you can use EDM to change your switch login user name or password.

Procedure steps

1. From the navigation menu, open **Configuration**, **Security**, **Control Path**.
2. Click **General**.
3. Click the **Web** tab.
   - Change the user name in the UserName field.
   - Change the password in the Password field.
4. Click **Apply**.

Configuring HTTP port number using EDM

Use this procedure to allocate a port, other than the default, for HTTP use.

Procedure steps

1. From the navigation menu, open **Configuration**, **Security**, **Control Path**
2. Click **General**.
3. Click the **Web** tab and enter a port number to use as the HTTP port.
4. Click **Apply**.

Configuring HTTPS mode using EDM

If you disable HTTPS mode and require secure connection to the switch over the Web, use the following procedure to re-enable the Web server secure-only option. Only HTTPS connections will be available. You can also use this procedure to allocate a port, other than the default, for HTTPS use.

Important:

Avaya strongly recommends that you discover the ports that UDP and TCP are already using before you select a port for HTTPS. Use the following commands to list the ports already in use and then select a port that is not in the resulting list.

For the CLI, use: `show ip tcp info-connections` and `show ip udp endpoints`.

For the ACLI, use: `show ip tcp connections`.

As a general recommendation, you should avoid using the ports between 1024-1100. Use ports 1100 and above.

Note:

When you change the default HTTPS port number while connected to EDM, you will lose connectivity. You can then reconnect to the switch using the new port number.

Procedure steps

1. From the navigation menu, open **Configuration**, **Security**, **Control Path**
2. Click **General**.
3. Click the **Web** tab and select the **SecureOnly** option.
4. Enter a port number to use as the HTTPS port.

The default port is 443.

5. Click **Apply**.

Installing EDM help files

While the EDM GUI is bundled with the software, the associated EDM help files are not included. To access the help files from the EDM GUI, you must install the EDM help files on a TFTP or FTP server in your network.

Use the following procedure to install the EDM help files on a TFTP or FTP server.

Do not install the EDM help files on PCMCIA or Flash.

Procedure steps

1. Retrieve the EDM help zip file from avaya.com or from the software CD.
2. On a TFTP or FTP server that is reachable from your switch, create a directory named: ERS8000_70_Help.

   Tip:

   Using FTP for data transfer:

   If you are using FTP for this installation, be sure that the switch is configured with the appropriate host name and password using the following commands:

   - For CLI:
     - `config bootconfig host user`
     - `config bootconfig host password`
   - For ACLI:
     - `boot config host user`
     - `boot config host password`

   Using TFTP for data transfer:

   If a host password is configured, the switch uses FTP to transfer data from the switch to the server.

   If no host password is configured, the switch uses TFTP for the data transfer. To clear the host password, specify a blank value using the host password command:

   - For CLI: `config bootconfig host password ""`
   - For ACLI: `boot config host password ""`
3. Unzip the EDM help zip file in the new FTP or TFTP server directory.

4. Using EDM on the switch, open the following folders: **Configuration** > **Security** > **Control Path**.
5. Double-click **General**.
6. Click the **Web** tab.
7. In the **HelpTftp/Ftp_SourceDir** field, enter the FTP or TFTP server IP address and the path of the online directory where the files are unzipped, in the following format: `<TFTP/FTP-server-IP-address>:ERS8000_70_Help`.
8. To test that the help is working properly, select any tab (for example, **Edit** > **Chassis**) and click the **Help** button.

   The appropriate EDM help page appears.

Selecting and launching a VRF Context view using EDM

Use this procedure to switch to another VRF Context view when you use the embedded EDM. GlobalRouter is the default view at log in.

You can configure both Global Router (GRT) and Virtual Routing and Forwarding (VRF) instances when you launch a VRF context view. The default view is text.

LIMITATION: you can open only 5 tabs per session.

Important:

If you log out from the GRT view, the system generates a warning: all tabs will be closed – and your session terminates. If you close a VRF view tab, you close only that view.

Note:

The Set VRF Context view function is not available to users in a service provider deployment where only a tenant VRF view is assigned. If you use a tenant VRF view, we recommend that you use the applicable EDM plugin with COM to access EDM. COM provides VRF mapping and Role-Based Access Control.

Procedure steps

1. From the navigation tree, select **Configuration** > **VRF Context view**.
2. Click **Set VRF Context view**.
3. Select a VRF ID from the list.
4. On the toolbar, click the **Launch VRF Context view** button.

   A new browser tab opens containing the selected VRF view.

Using the chassis shortcut menu

Use the following procedure to display the chassis shortcut menu.

Procedure steps

1. In the Device Physical View, select the chassis and right-click.
2. For more information, see the following Variable definitions table.

Variable definitions

The following table shows the field descriptions for the Chassis shortcut menu.

Variable	Value
Edit	Edit chassis parameters.
Graph	Graph chassis statistics.
Refresh Port Tooltip	Refresh the port tooltip data of the switch. The port tooltip data contains: Slot/Port, PortName, and PortOperSpeed.

Using the card shortcut menu

The card or module shortcut menu provides a quick way to view the card parameters. This shortcut menu is context-sensitive and based on the currently selected card type.

Procedure steps

1. In the Device Physical View, select a module and right-click.
2. If the selected card is an I/O module, click **Edit**.

Using the port shortcut menu

Use the following procedure to display the port shortcut menu.

Procedure steps

1. In the Device Physical View, select a port and right-click.
2. For more information, see the following Variable definitions table.

Variable definitions

Use the data in the following table to use the fields for the Port shortcut menu.

Field	Description
Edit General	Displays the edit port menu.
Edit IP	Displays the edit IP port menu.
Edit IPv6	Displays the edit IPv6 port menu.
Graph	Graphs the port statistics.
Enable	Administratively brings a port up.
Disable	Administratively shuts down a port.

Opening folders and tabs

Use the following procedure to navigate around EDM.

Procedure steps

1. In the navigation pane, open the navigation tree by clicking on the arrowhead located to the left of the **Configuration** folder.

This action displays the top-level folders in the tree such as **Edit**, **Graph**, and **VLAN**.

2. If there is a subfolder such as the **Spanning Tree** subfolder under **VLAN**, click on that arrowhead to open the folder.
3. Under the folders and subfolders are the primary tabs, open them by double-clicking on the tab.

Undocking and docking tabs

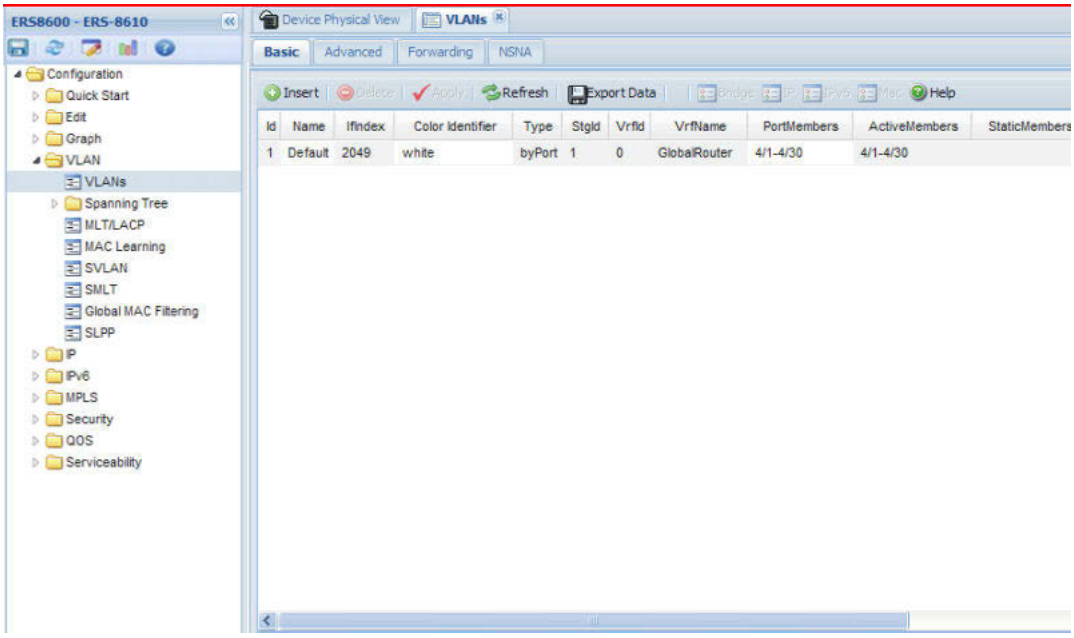
Use this procedure to compare the dialog box that you are configuring with a dialog box from another tab. This undocking feature enables you to view screens side-by-side so that you can see information that you need from another tab.

The following example shows the VLANs Basic tab in the background so you can reference it while you are configuring Port 4/1.

Procedure steps

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

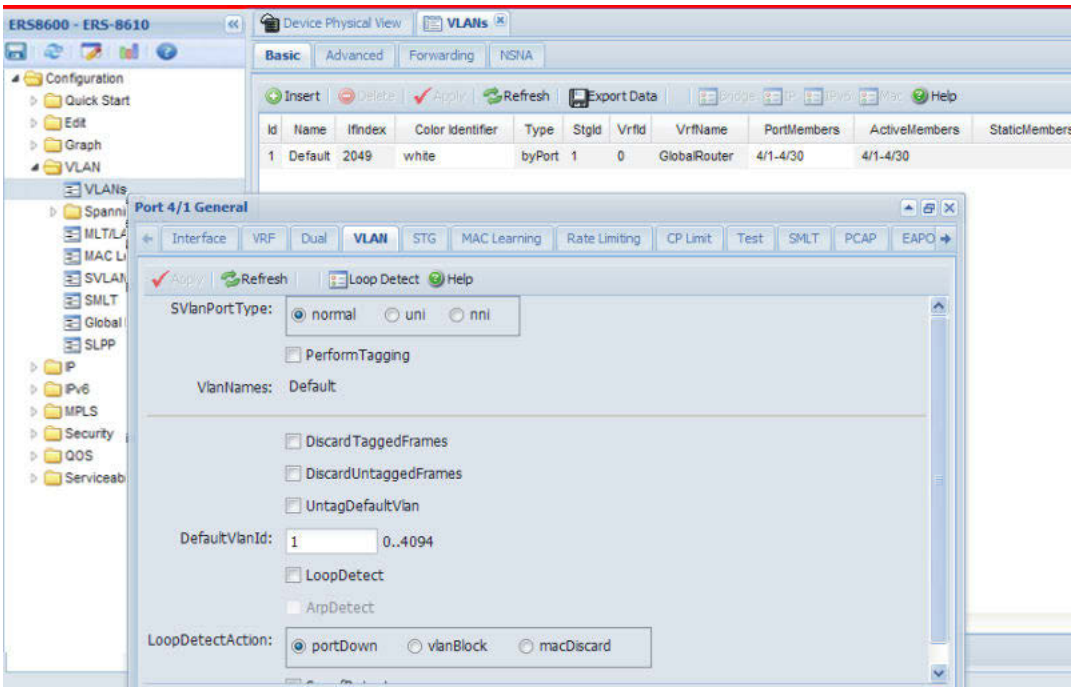
   The **VLANs** tab appears in the menu bar and the **Basic** dialog box displays in the work area as shown in the following figure.



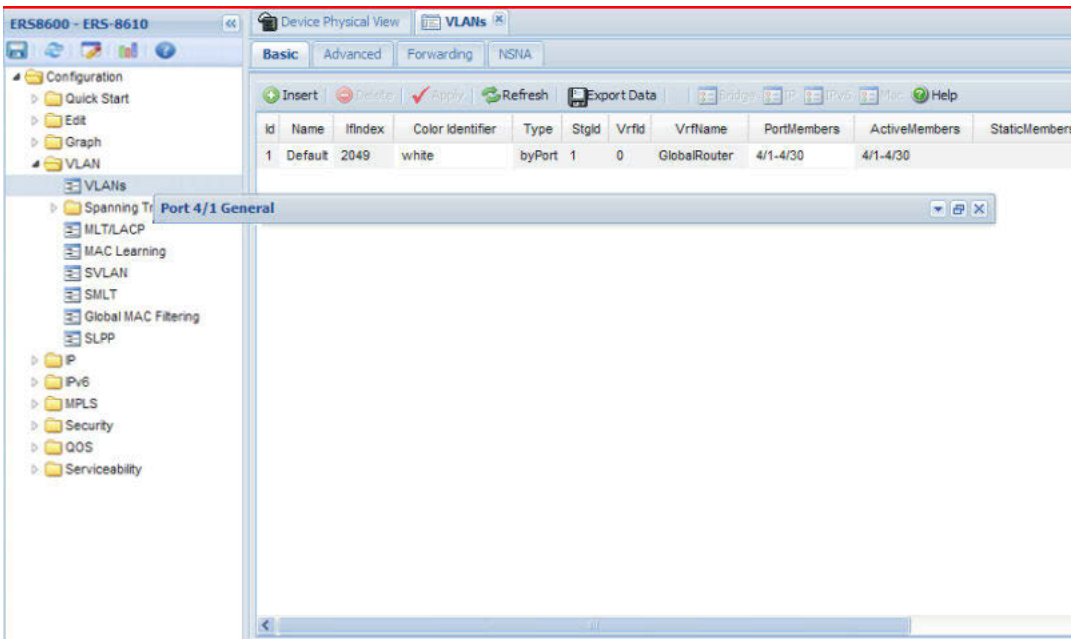
3. In the Device Physical View, select a port. In this example, right-click port 1 in slot 4.
4. Click **Edit General**.

The **Port 4/1 General** tab appears in the menu bar and the **Interface** dialog box displays in the work area.

5. Click **VLAN** to display the VLAN dialog box for port 4/1.
6. Click and drag the **Port 4/1 General** tab wherever you want on the screen as shown in the following figure.



7. To reposition the dialog box anywhere on the screen, click and drag the title bar.
8. To manipulate the dialog box, click on the buttons in the top-left of the dialog box.
9. Click the **up arrowhead** button to minimize the dialog box as shown in the following figure.



10. Click the **down arrowhead** button to restore the dialog box to its original size.
11. Click the **pages** button to dock the dialog box back into the menu bar.
12. Click the **X** button to close the dialog box.

Editing objects

You can edit objects and values in EDM in four ways.

Procedure steps

1. To edit objects and values, do one of the following:
   - Select an object. From the EDM toolbar, click **Edit Selected**.
   - From the shortcut menu for a chassis, module, port, or any other object, select **Edit**.
   - Double-click the object.

   After you change values in a field, the changes you make appear in bold.
2. Click **Apply** to apply the changes to the device.
3. After you apply changes to fields, click **Refresh** to display the new information in the tab or dialog box.
4. To make changes in the running configuration, click **Apply**.

   Important:

Changes are not applied to EDM until you click Apply.

5. Open the **Configuration** > **Edit** > **Chassis** folders.
6. In the **ActionGroup1** section of the **System** dialog box, click **saveRuntimeConfig** to make the changes permanent.

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 user-determined values. For example, the value for a system contact is a name you enter in the **SysContact** field. Editable fields in EDM dialog boxes appear in white.

Procedure Steps

1. Double-click the field and select the drop-down icon.

   The choices for that parameter appear.
2. Click a new value from the list.
3. For fields without preset values, double-click the field and enter the value.
4. Click **Apply**.

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. Multiple time formats and calculations exist, depending on the feature.

See the following table for EDM dialog box button descriptions.

EDM dialog box buttons

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

Table 10: EDM 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 and displays new information.
Close	Close the tab or dialog box and disregard changes you made to fields.
Help	Open context-sensitive Online Help.
Resize Columns	Resize table columns to fit the data in them.
Stop	Stop the current action (polling).
Export data	Copy data to external media.
Graph	Graph selected data. For more information about graphing, see *Performance Management,* NN46205-704.
Export (on Graph dialog boxes)	Save the current table in ASCII format in a file you specify. The table contains tabs that you use to import this file into a text editor or spreadsheet for further analysis.
Print (on Graph dialog boxes)	Print the current table.
Clear Counters	Clears the existing number of counters and restarts them.
Clear All	Clears the numbers for all statistics and restarts the count.

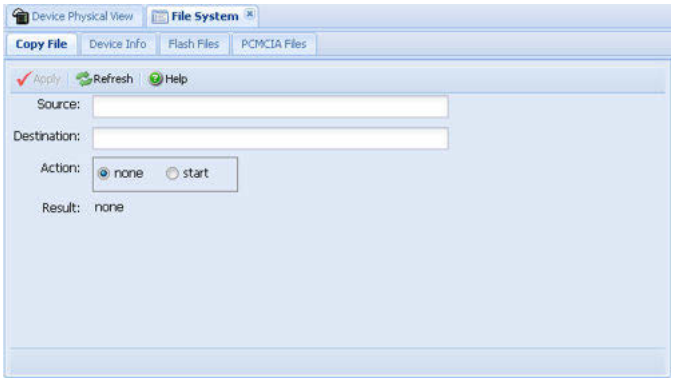
Copying files

Use the following procedure to copy a file.

Procedure steps

1. In the navigation tree, open the **Configuration** > **Edit** folders.
2. Double-click **File System**.

   The **File System** tab appears with the **Copy File** tab displayed.



3. In the **Source** field, specify the file you want to copy in one of the following forms:
   - `/flash/filename`
   - `/pcmcia/filename`
   - `ipaddress:/home/user/filename`
4. In the **Destination** field, specify the location where you want to copy the file in one of the following forms:
   - `/flash/filename`
   - `/pcmcia/filename`
   - `ipaddress:/home/user/filename`
5. In the **Action** field, click **start**.
6. Click **Apply** to start copying the files.

   The results of the action appear in the **Result** field.

Example of copying files:

To copy a configuration file to a remote TFTP server,

1. Enter `10.10.40.20:/home/joe/config.cfg` in the Destination box
2. Enter `/flash/config.cfg` in the Source box.

Viewing files on the device

You can view information about the flash and PCMCIA memory such as the number of bytes used and the number of bytes free. The slot number indicates the chassis location of the referenced SF/CPU.

Procedure steps

1. In the navigation tree, open the **Configuration** > **Edit** folders.
2. Double-click **File System**.

The **File System** tab opens with the **Copy File** dialog box displayed.

3. Click **Device Info**.

Viewing file data on the Flash memory

You can view the name, modification date, and size of each switch file in the onboard flash memory. The slot number indicates the chassis location of the referenced SF/CPU.

Procedure steps

1. In the navigation tree, open the **Configuration** > **Edit** folders.
2. Double-click **File System**.

   The **File System** tab opens with the **Copy File** dialog box displayed.
3. Click **Flash Files**.

Viewing file data on the PCMCIA card

You can view the names, modification date, and size of each switch file in the PCMCIA module. The slot number indicates the chassis location of the referenced SF/CPU.

Procedure steps

1. In the navigation tree, open the **Configuration** > **Edit** folders.
2. Double-click **File System**.

   The File System tab opens with the **Copy File** dialog box displayed.
3. Click **PCMCIA Files**.

Setting EDM access parameters using EDM

You can use Enterprise Device Manager to configure access parameters, including passwords.

Procedure steps

1. From the navigation menu, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Web** tab.
4. Use the **UserName** and **Password** fields to specify the user name and password for access to Enterprise Device Manager.

   Note that rwa is the access level provided to the Web/EDM user, regardless of the user name you choose.

Variable definitions

Use the data in the following table to use the Web tab.

Variable	Value
UserName	Specifies the user name for the Enterprise Device Manager account.
Password	Specifies the password for the Enterprise Device Manager account.
HelpTftpSourceDir	Specifies the TFTP source directory for Help files.
DefaultDisplayRows	Specifies the default display rows for the HTML pages.
LastChange	Specifies the time of the most recent change to the switch configuration using the Web interface. This field always reads none.
NumHits	Specifies the number of times pages in the Web interface are accessed.
NumAccessChecks	Specifies the number of times access attempts are authenticated.
NumAccessBlocks	Specifies the number of times access is attempted and denied.
LastHostAccessBlocked	Specifies the last host accessed blocked.
NumRxErrors	Specifies the number of receive errors.
NumTxErrors	Specifies the number of transmit errors.
NumSetRequest	Specifies the number of set-requests sent to the Web server.

Multiple port monitoring and configuration support

When you want to monitor or apply the same configuration changes to more than one port, you can use the Multiple Port Selection function. You can use the standard menus and the shortcut menus with Multiple Port selection. If you use the embedded EDM, you can select up to a maximum of 24 ports. There is no port limitation for COM users.

On the Device Physical View, using a standard mouse, you can either

- Ctrl+click to select up to 24 specific ports (for the embedded EDM)
- click and drag to select up to 24 adjacent ports (for the embedded EDM)

If you use click and drag, ensure that you click just outside the first port in the group and drag the mouse pointer over the group. Selected ports for both methods appear within a yellow outline on the Device Physical View.

Using Multiple Port Selection and the shortcut menu

Use the following procedure to use the port shortcut menu to configure up to 24 ports at once for the embedded EDM; there is no limitation for COM.

Procedure steps

In the Device Physical View, do one of the following if you are using a standard mouse.

a. To select several ports, point your mouse to each port and use Ctrl+Click to select up to 24 ports.

   The selected ports appear within a yellow outline on the Device Physical View.

   i. Right click your mouse to display the shortcut menu.

   ii. Select an option from the shortcut menu.

b. To select a group of adjacent ports, point your mouse just outside the group and drag the pointer over the group (embedded EDM is limited to selection of a maximum of 24 ports at once).

   The selected ports appear within a yellow outline on the Device Physical View.

   Right click your mouse to display the shortcut menu.

Select an option from the shortcut menu.

Variable definitions

The information in the following table describes the options in the shortcut menu.

Variable	Value
Edit General	Displays the Configuration, Edit, Port tabs, with the Interface tab open, for only the selected ports.
Edit IP	Displays the Configuration, Edit, Port, IP tabs, with the IP Address tab open, for only the selected ports.
Edit IPv6	Displays the Configuration, Edit, Port, IPv6 tabs for only the selected ports.
Graph	Displays the Configuration, Graph, Port tabs, with the Interface tab open so you can graph statistics for the selected ports. For more information about graphing, see *Performance Management (NN46205-704).*
Enable	Administratively brings the selected ports up. A warning box appears and you must select **Yes** to enable the ports.
Disable	Administratively shuts down the selected port ports. A warning box appears and you must select **Yes** to shut the ports down.

Configuring Status Polling

Use this procedure to configure when to update the LED/Port status.

Procedure steps

1. From the navigation menu, open **Configuration** > **Device** > **Preference Setting**.
2. Click **Enable** under **Status Polling**.
3. Select a poll interval from the options available.
4. Click **Apply**.

Configuring Hot Swap Detection

Use this procedure to detect when modules are removed from or inserted into the switch.

Procedure steps

1. From the navigation menu, open **Configuration** > **Device** > **Preference Setting**.
2. Click **Enable** under **Hot Swap Detection**.
3. Select an interval from the options available next to **Detection per Status Poll Intervals**.
4. Click **Apply**.