Using CLI and EDM

Release 4.3
NN47500-101
Issue 01.01
March 2016

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Contents

Chapter 1: New in this document

Using CLI and EDM is a new document for Release 4.3 so all the features are new in this release. See *Release Notes* for a full list of features.

Chapter 2: Command line interface fundamentals

This section describes the command line interface (CLI).

CLI is an industry standard command line interface that you can use for single-device management.

CLI command modes

CLI has six major command modes in this release. You start your session on the switch in User EXEC mode. From User EXEC mode, you can enter Privileged EXEC mode. From Privileged EXEC mode, you can enter Global Configuration mode. From Global Configuration mode, you can enter one of the remaining modes.

Each mode provides a specific set of commands. While in a higher mode, you can access most commands from lower modes, except if they conflict with commands of your current mode.

The following list describes the command modes:

- User EXEC mode—the initial mode of access. Only a limited number of commands are available in the User EXEC mode. Most EXEC commands are one-time commands, such as show commands, which show the current configuration status. The EXEC commands are not saved across restarts.
- Privileged EXEC mode—access this mode from the User EXEC mode. The user name and password combination determines your access level in the Privileged EXEC mode and higher modes. Enter **`enable`** to access this mode from the User EXEC mode. As with the User EXEC mode commands, most EXEC commands are one-time commands, such as show commands, which show the current configuration status. The Privileged EXEC mode commands are also not saved across restarts.
- Global Configuration mode—access this mode from the Privileged EXEC mode. Enter **`config {terminal|network}`** to access the Global Configuration mode. Use this mode to make changes to the running configuration. If you save the configuration, these settings survive a restart of the system.
- Interface Configuration mode—access this mode from the Global Configuration mode.

Note:

The **mgmtEthernet mgmt** command applies only to hardware with a dedicated, physical management interface.

Enter **interface {GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}> | loopback <1-256> | mgmtEthernet mgmt | mlt <1-512> | vlan <1-4059>}** to access the Interface Configuration mode. 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 or slot. You can configure the following interfaces:

- GigabitEthernet
- Loopback
- mgmtEthernet
- MLT
- VLAN

- Router Configuration mode—access this mode from the Global Configuration mode. Enter **router {bgp|isis|ospf|rip|vrf WORD<1-16> | vrrp}** to access the Router Configuration mode. Use this mode to modify a protocol. You can configure the following protocols:
  - BGP
  - IS-IS
  - OSPF
  - RIP
  - VRF
  - VRRP
- Application Configuration mode—access this mode from the Global Configuration mode. Enter application to access the Application Configuration mode.

From either the Global Configuration mode or the Interface Configuration mode, you can save all of the configuration parameters to a file. The default name for the configuration file is config.cfg. You can also use alternative file names.

You can enter most of the show commands from the User EXEC mode. In most cases, you can also enter the show commands in all of the upper-level command modes.

The following table lists the CLI command modes, the prompt for each mode, and explains how to enter and exit each mode. The prompt is prefaced by the system name, for example:

- `Switch:1#`
- `Switch:1(config-bgp)#`
- `Switch:1>`
- `Switch:1(config-if)#`

Table 1: CLI command modes

Command mode	Prompt	Command mode or enter/exit mode
User EXEC	>	This mode is the default command mode and does not require an entrance command. To exit the CLI, enter **logout**.
Privileged EXEC	#	Enter **enable** to access the Privileged EXEC mode from the User EXEC mode. Enter **disable** to exit the Privileged EXEC mode, and enter the User EXEC mode. To exit the CLI, enter **logout**.
Global Configuration	(config)#	From the Privileged EXEC mode, enter **configure**, followed by either **terminal** or **network** to access the Global Configuration mode. Enter **exit** to exit the Global Configuration mode, and enter the Privileged EXEC mode. To exit the CLI, enter **logout**.
Interface Configuration	(config-if)# (config-mlt)#	Entry into this command mode depends on the type of configured interfaces. From the Global Configuration mode, enter **interface {GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}> | loopback <1-256> | mgmtEthernet mgmt | mlt <1-512> | vlan <2-4059>}** to access the Interface Configuration mode. Enter **exit** to exit the Interface Configuration mode and enter the Global Configuration mode. To return to the Privileged EXEC mode, enter **end**. To exit the CLI, enter **logout**. **Note:** The **mgmtEthernet mgmt** command applies only to hardware with a dedicated, physical management interface.
Router Configuration	(config-bgp)# (config-isis)# (config-ospf)# (config-rip)# (router-vrf)# (config-vrrp)#	Entry into this command mode depends on the configured protocols. Enter **router {bgp|isis|ospf|rip|vrf WORD<1-16> | vrrp}** to access the Router Configuration mode from the Global Configuration mode. Enter **exit** to exit the Router Configuration mode and enter the Global Configuration mode. To return to the Privileged EXEC mode, enter **end**. To exit the CLI, enter **logout**.
Application Configuration	(config-app)#	Enter application to access the Application Configuration mode from the Global Configuration mode. Enter exit to exit the Application Configuration mode, and enter the Global Configuration mode. To return to the Privileged EXEC mode, enter end. To exit the CLI, enter logout.

Default user names and passwords

The following table contains the default user names and passwords that you can use to log on to the switch using the command line interface (CLI). For more information about how to change passwords, see *Configuring Security*.

Table 2: CLI default user names and passwords

User name	Password	Description
rwa	rwa	read-write-all
rw	rw	read-write
ro	ro	read-only
l1	l1	layer 1
l2	l2	layer 2
l3	l3	layer 3

If you enable enhanced secure mode, the user names and passwords are different than the default values documented in the preceding table. For more information on enhanced secure mode, see *Administering*.

Important:

The default passwords and community strings are documented and well known. It is strongly recommended 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*.

Documentation convention for the port variable

Commands that require you to enter one or more port numbers on the switch use the parameter {slot/port[/sub-port][-slot/port[/sub-port]][,...]} in the syntax. The following list specifies the rules for using {slot/port[/sub-port][-slot/port[/sub-port]][,...]}.

- {slot/port[/sub-port]} — Identifies a single slot and port. If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. For example, 1/1 indicates the first port on slot 1. 1/41/1 indicates the first channel on slot 1, port 1.
- {slot/port[/sub-port][-slot/port[/sub-port]][,...]}— Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. For example, 1/1–1/3 indicates ports 1 to 3 on slot 1, or 1/41/1,1/41/3 indicates the first and third channels of slot 1, port 41.

Command completion

The CLI provides potential command completions to the command string. Completions are provided by using a **?** or by using the CLI autocompletion feature:

- Question mark (**?**)
- CLI autocompletion

? command completion

The **?** command completion is available for any valid command. By typing a command and using a **?** as the last argument in the command, the system returns a list of possible command completions from the point of the **?**. A short description is provided with each possible completion.

Example

If you enter the following command:

```
Switch:1(config-isis)#redistribute ?
```

CLI provides a list of completions for the **`redistribute ?`** command.

```
Switch:1(config-isis)#redistribute ?
    direct     isis redistribute direct command
    ospf        isis redistribute ospf command
    rip          isis redistribute rip command
    static     isis redistribute static command
```

All the parameters listed under redistribute indicate sub-context commands.

You must use one of the available completions, and if necessary, use the command completion help again to find the next completion.

```
Switch:1(config-isis)#redistribute direct ?
  enable       Enable isis redistribute direct command
  metric       Isis route redistribute metric
  metric-type  Set isis redistribute metric type
  route-map    Set isis redistribute direct route-policy
  subnets      Set isis redistribute subnets
<cr>
```

When you see <cr> (Carriage Return/Enter Key) in the list with the additional choices, this means that no additional parameters are required to execute the CLI command. However, the additional choices listed could be peer commands or sub-context commands.

For example, the parameters listed under **`redistribute direct ?`** are peer commands. You can enter these peer commands on the same line as the root command, for example, **`redistribute direct enable`**. However, the <cr> indicates that you can enter only the **`redistribute direct`** command. You do not require any additional parameters at this level.

CLI autocompletion

CLI autocompletion is a feature that you can use to automatically fill in the unique parts of a command string rather than typing the entire command. Autcompletion makes the CLI experience easier and prevents mistakes in spelling that force you to re-enter the command.

Autocompletion completes the token in the command as soon as it becomes unique.

The **Tab** key autocompletes the command without running the command, and places the cursor immediately after the last character. The **Enter** key autocompletes the command and then runs it.

Example

To enable redistribution of isis direct routes,

```
Switch:1(config-isis)#redistribute direct
```

When you use **`redistribute ?`**, you see the following four possible sub-context commands:

```
direct
static
ospf
rip
```

If you type the following without pressing **Enter**:

```
Switch:1(config-isis)#redistribute direct m
```

and press the **Tab**, the system completes the command to the following point:

```
redistribute direct metric
```

Two possible completions exist. You can type **-t**, and then press **Tab** to finish the command:

```
Switch:1(config-isis)#redistribute direct metric-type
```

Chapter 3: CLI procedures

This chapter contains information about common CLI tasks. You can access CLI during runtime to manage the switch.

Logging on to the software

Before you begin

- The first time you connect to the switch, you must log on to CLI using the direct console port.

About this task

After you first connect to CLI you can log on to the software using the default user name and password. For more information about the default user names and passwords, see Default user names and passwords on page 10.

Procedure

1. At the login prompt, enter the user name.
2. At the password prompt, enter the password.

Viewing configurations

You can view the running configuration using the show command.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View running configuration:

   ```
   show running-config
   ```

Example

The following example uses a generic variable for the hardware information. The output on your system will be more specific.

```
Switch:1#show running-config
Preparing to Display Configuration...
#
#
# Thu Feb 05 18:38:02 2016 UTC
# box type             : ProductNameX
# software version     : 4.3.0.0GA
# cli mode             : CLI
#
#

#
#!end

#
config terminal
#
#
#BOOT CONFIGURATION
#

boot config flags ftpd
boot config flags telnetd
# end boot flags
auto-recover-delay 10

#CLI CONFIGURATION
#

telnet-access sessions 3
password password-history 3

#
#SYSTEM CONFIGURATION
#

ip name-server primary 10.1.1.1
sys msg-control control-interval 30
sys msg-control

#
#
```

Changing user modes in CLI

Perform this procedure to change user modes in CLI.

Before you begin

- You must log on to CLI.

About this task

You can enter shortened versions of the commands, if the letter combination is unique.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Access the Interface Configuration mode:

   Note:

   The **mgmtEthernet mgmt** command applies only to hardware with a dedicated, physical management interface.

   ```
   interface {GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} | loopback <1-256> | mgmtEthernet mgmt|mlt <1-512> | vlan <1-4059>}
   ```

3. Access the Router Configuration mode:

   ```
   router {bgp [0-65535] | isis [enable] | ospf [enable|ipv6-enable] | rip [enable [vrf <1-511>]] | vrrp}
   ```

4. Access the Application Configuration mode:

   ```
   application
   ```

Example

Access Privileged EXEC mode:

```
Switch:1>enable
```

Access Global Configuration mode:

```
Switch:1#configure terminal
```

Access Interface Configuration mode for a VLAN:

```
Switch:1(config)#interface vlan 2
```

Access Router Configuration mode for BGP:

```
Switch:1(config-if)# router bgp
```

Exit back to Global Configuration mode:

```
Switch:1(router-bgp)# exit
```

Access Router Configuration mode for isis:

```
Switch:1(config-if)#router isis
```

Exit back to Global Configuration mode:

```
Switch:1(config-isis)#exit
```

Access Router Configuration mode for OSPF:

```
Switch:1(config)#router ospf
```

Exit back to Global Configuration mode:

```
Switch:1(router-ospf)#exit
```

Access Application Configuration mode:

```
Switch:1(config)# application
```

Exit back to Privileged EXEC mode:

```
Switch:1(config-app)# end
```

Exit back to User EXEC mode:

```
Switch:1#disable
```

Exit the system:

```
Switch:1>exit
```

Variable definitions

Use the data in the following table to use the **`interface`** command.

Variable	Value
GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Logs on to the GigabitEthernet Interface Configuration mode. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
loopback <*1-256*>	Logs on to the loopback Interface Configuration mode. Use <*1-256*> to specify which interface to configure.
mgmtEthernet *mgmt* **Note:** The mgmtEthernet mgmt command applies only to hardware with a dedicated, physical management interface.	Logs on to the mgmtEthernet Interface Configuration mode. Use *mgmt* for management configurations.
mlt <*1-512*>	Logs on to the multi-link trunking (MLT) Interface Configuration mode. Use <*1-512*> to specify which MLT to configure.
vlan	Logs on to the Virtual Local Area Network (VLAN) Interface Configuration mode. Use <*1-4059*> to specify which VLAN to configure.

Use the data in the following table to use the **`router`** command.

Variable	Value
isis [enable]	Enter IS-IS Router Configuration mode. The command **`router isis`** allows you to enter IS-IS Router Configuration mode. After the configuration, use **`router isis enable`** to enable IS-IS globally.
ospf	Enter OSPF Router Configuration mode. The command **`router ospf`** allows you to enter OSPF Router Configuration mode. After the configuration, use **`router ospf enable`** to enable OSPF globally.
rip	Enter RIP Router Configuration mode. The command **`router rip`** allows you to enter RIP Router Configuration mode. After the configuration, use **`router rip enable`** to enable RIP globally.
vrf *WORD<1-16>*	Enter Virtual Router Forwarding (VRF) Router Configuration mode. Specify the VRF name to configure. The command **`router vrf WORD<1-16>`** allows you to enter VRF Router Configuration mode.
vrrp	Enter Virtual Router Redundancy Protocol Router Configuration mode.

Saving the configuration

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

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) supports both IPv4 and IPv6 addresses.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

```
Switch:1> enable
```

Save the configuration to the default location:

```
Switch:1# save config
```

Identify the file as a backup file and designate a location to save the file:

```
Switch:1# save config backup 46.140.54.40/configs/backup.cfg
```

Variable definitions

Use the data in the following table to use the **`save config`** command.

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following formats: • a.b.c.d:<file> • /intflash/<file> The file name, including the directory structure, up to 1 to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following formats: • /intflash/<file> • a.b.c.d:<file> The file name, including the directory structure, up to 1 to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Chapter 4: Enterprise Device Manager fundamentals

The following section provides details about Enterprise Device Manager (EDM).

EDM is a web-based GUI that you can use to configure a single switch. EDM runs from the switch and you can access it from a web browser. You do not need to install additional client software, and you can access it with all operating systems.

Supported browsers

Use the following recommended browser versions to access Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 11
- Mozilla Firefox 43+

Note:

The following earlier browser versions can be used to access EDM (although not recommended):

- Microsoft Internet Explorer 9 and 10
- Mozilla Firefox 37 through 40

Enterprise Device Manager access

To access EDM, open *http://<IP_address>* or *https://<IP_address>* from either Microsoft Internet Explorer or Mozilla Firefox. Ensure you use a supported browser version.

Important:

- You must enable the web server from CLI to enable HTTP access to the EDM. If you want HTTP access to the device, you must also disable the web server secure-only option. The web server secure-only option, allowing for HTTPS access to the device, is enabled by default. It is recommended that you take the appropriate security precautions within the

network if you use HTTP. For more information about enabling the web server from CLI, see Configuring the web server using CLI on page 26.

- EDM access is available to read-write users only.

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

Default user name and password

The following table contains the default user name and password that you can use to log on to the switch using EDM.

Table 3: EDM default username and password

Username	Password
admin	password

Important:

The default passwords and community strings are documented and well known. It is strongly recommended 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*.

Device Physical View

After you access EDM, the system displays a real-time physical view of the front panel of the device. From the front panel view, you can view fault, configuration, and performance information for the device or a single port. You can open this tab by clicking the Device Physical View tab above the device view.

You can use the device view to determine the operating status of the various ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects. In the device view, you can select a port or the entire chassis. To select an object, click the object. EDM outlines the selected object in yellow, indicating your selection.

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

EDM window

The following figure shows the different sections of the EDM window:

- Navigation pane—Located on the left side of the window, the navigation pane displays all the available command tabs in a tree format. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.
- Menu bar—Located at the top of the window, the menu bar shows the most recently accessed primary tabs and their respective secondary tabs.
- Toolbar—Located just below the menu bar, the toolbar gives you quick access to the most common operational commands such as Apply, Refresh, and Help.
- Work area—Located on the right side of the window, the work area displays the dialog boxes where you can view or configure parameters on the switch.

The following figure shows an example of the Device Physical View window.

Note:

The Device Physical View on your hardware type can appear differently than the following example.

Figure 1: EDM window

Navigation pane

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

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

Table 4: 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 pane.

Table 5: Navigation pane folders

Menu	Description
Device	Use the Device menu to refresh and update device information or enable polling. • 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.
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 port. 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.

Table continues…

Menu	Description
VLAN	Use the VLAN menu to view and configure VLANs, spanning tree groups (STG), MultiLink Trunks/LACP, SMLT, and SLPP.
IS-IS	Use the IS-IS menu to view and configure IS-IS, Shortest Path Bridging MAC (SPBM) and statistics.
IP	Use the IP menu to view and configure IP routing functions for the system, including TCP/UDP, OSPF, RIP, VRRP, RSMLT, DHCP Relay, UDP forwarding, IS-IS and Policy.
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.

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 can open from the navigation pane. These primary tabs appear in the sequence that you open them.
- After you click a primary tab, the system displays the associated secondary tabs in the bottom row. Click a secondary tab to open it in the work area.

In both the top and bottom rows of the menu bar, if the number of tabs exceeds the available space on the desktop, the system displays left- and right-pointing arrows. Click an arrow to scroll to the required tab.

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

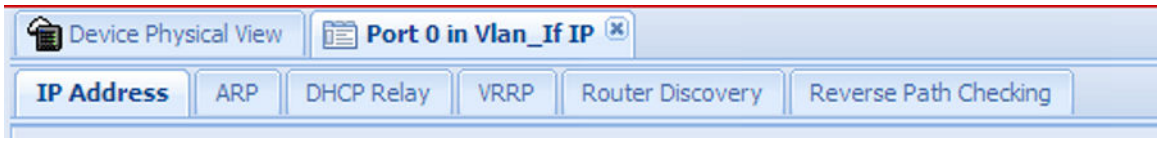


Figure 2: Menu bar

Toolbar

The toolbar buttons provide quick access to commonly used operational commands. The buttons vary depending on the tab that you select. However, the Apply, Refresh, and Help buttons are on

almost every screen. Other common buttons are Insert and Delete. The following list provides the details for the common toolbar buttons.

- Apply—Use this button to execute all changes that you make.
- Refresh—Use this button to refresh all data on the screen.
- Help—Use this button to display context-sensitive online help 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 in the dialog box. This causes a new entry to appear in the dialog box of the selected tab.
- Delete—Use this button to delete a selected entry.

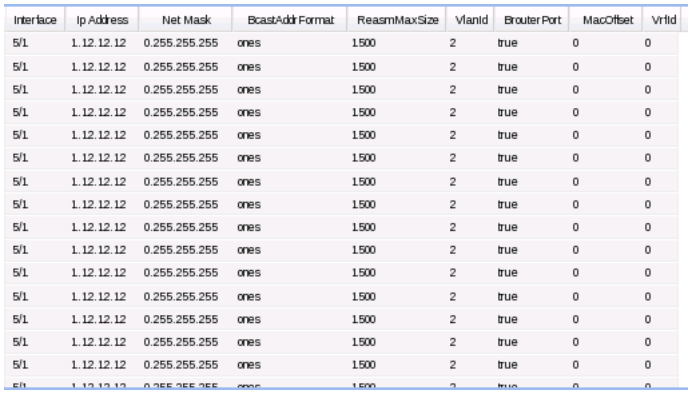
The following figure shows a sample toolbar.

Figure 3: Toolbar

Work area

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

The following figure is a sample work area showing the dialog box for the Port 1/3 General, Interface tab. If you want to compare the information in two dialog boxes, you can undock one, then open another tab. For more information about undocking a tab, see Undocking and docking tabs on page 32.



Interface	Ip Address	Net Mask	BcastAddrFormat	ReasmMaxSize	VlanId	BrouterPort	MacOffset	VrfId
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0
5/1	1.12.12.12	0.255.255.255	ones	1500	2	true	0	0

Figure 4: Work area

EDM user session extension

If the EDM user session remains unused for a duration of 10 minutes, the system displays the following message:

Your session will expire in about 5 minute(s). Would you like to extend the session?

If the user does not respond, EDM automatically ends the session with the following message: *Your session has expired.*

The user can log on again if they want to continue to use EDM.

Chapter 5: EDM interface procedures

This chapter contains procedures for starting and using Enterprise Device Manager (EDM). The software is built-in to the switch, and you do not need to install additional software.

Configuring the web server using CLI

Perform this procedure to enable and manage the web server using the command line interface (CLI). After you enable the web server, you can connect to EDM.

HTTP and FTP support both IPv4 and IPv6 addresses, with no difference in functionality or configuration. The TFTP server supports both IPv4 and IPv6 addresses. The TFTP client is not supported, only the server.

About this task

This procedure assumes that you use the default port assignments. You can change the port number used for HTTP.

Important:

If you want to allow HTTP access to the device, then you must disable the web server secure-only option.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the web server:

   ```
   web-server enable
   ```

3. Display the web server status:

   ```
   show web-server
   ```

Variable definitions

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

Variable	Value
def-display-rows *<10-100>*	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the web interface. To disable the web server, use the no form of this command: `no web-server [enable]`
help-tftp *WORD<0-256>*	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths show the correct format: • 47.17.82.25:/help • 47.17.82.25:/
http-port *<80 | 1024-49151>*	Configures the web server HTTP port. The default port is 80.
https-port *<443 | 1024-49151>*	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout*<30–65535>*	Configures the web-server login session inactivity timeout. The value is in seconds.
password {ro | rw | rwa} *WORD<1-20> WORD<1-20>*	Configures the logon and password for the web interface, where the first *WORD<1-20>* is the new logon and the second *WORD<1-20>* is the new password.
secure-only	Enables secure-only access for the web server.

Connecting to EDM

Use the following procedure to connect to EDM to configure and maintain your network through a GUI.

Before you begin

- Ensure that the switch is running.
- Note the IP address of the switch.
- Ensure you use a supported browser version.

Procedure

1. In the address field, enter the IP address of the system using the following formats: **https://<IP_address>** (default) or **http://<IP_address>**.

   Note:

   By default the web server is configured with the secure-only option, which requires you to use HTTPS to access EDM. To access EDM using HTTP, you must disable the

secure-only option. For more information about configuring the secure-only option, see Configuring the web server using CLI on page 26.

2. In the **User Name** field, type the user name. The default is admin.
3. In the **Password** field, type a password. The default is password.
4. Click **Log On**.

   For information about changing the Log On credentials, see *Configuring Security*.

Configuring the web management interface

Before you begin

- The Web server is enabled.

About this task

Configure the web management interface to change the usernames and passwords for management access to the switch using a web browser.

HTTP, FTP, and TFTP server supports both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Web** tab.
4. Complete the **WebUserName** and **WebUserPassword** fields to specify the user name and password for access to the web interface. You use the other fields to specify the path and file name for the web Help files and to assign the number of rows in the web display.
5. Click **Apply**.

Web field descriptions

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

Name	Description
HttpPort	Specifies the HTTP port for web access. The default value is 80.
WebUserName	Specifies the username from 1–20 characters. The default is admin.

Table continues…

Name	Description
WebUserPassword	Specifies the password from 1–20 characters. The default is password.
SecureOnly	Controls whether the secure-only option is enabled. The default is enabled.
HelpTftp/Ftp_SourceDir	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/| peer:/ [<dir>]. The path can use 0–256 characters. The following example paths show the correct format: • 47.17.82.25:/help • 47.17.82.25:/
DefaultDisplayRows	Configures the web server display row width between 10–100. The default is 30.
LastChange	Shows the last web-browser initiated configuration change.
NumHits	Shows the number of hits to the web server.
NumAccessChecks	Shows the number of access checks performed by the web server.
NumAccessBlocks	Shows the number of access attempts blocked by the web server.
LastHostAccessBlocked	Shows the IP address of the last host access blocked the web server.
NumRxErrors	Shows the number of receive errors the web server encounters.
NumTxErrors	Shows the number of transmit errors the web server encounters.
NumSetRequest	Shows the number of set-requests sent to the web server.

Using the chassis shortcut menu

About this task

Perform the following procedure to display the chassis shortcut menu.

Procedure

1. In the Device Physical View, select the chassis.
2. Right-click the chassis.

Chassis shortcut menu field descriptions

Use the data in the following table to use the Chassis shortcut menu.

Name	Description
Edit	Edits chassis parameters.
Graph	Graphs chassis statistics.
Refresh Status	Refreshes the status of the chassis.
Refresh Port Tooltips	Refreshes the port tooltip data of the system. The port tooltip data contains the following variables: Slot/Port, PortName, and PortOperSpeed.

Using the port shortcut menu

About this task

Perform this procedure to display the port shortcut menu.

Procedure

1. In the Device Physical View, select a port.
2. Right-click the selected port.

Port shortcut menu field descriptions

Use the data in the following table to use the port shortcut menu.

Name	Description
Edit General	Configures the general options for the port.
Edit IP	Configures the IP options for the port.
Edit IPv6	Configures the IPv6 options for the port.
Graph	Displays the statistics for the port.
Enable	Enables the port.
Disable	Disables the port.

Using a table-based tab

The following procedure provides an example about how to use a table-based tab.

About this task

Change an existing configuration using a table-based tab. You cannot edit gray-shaded fields in the table.

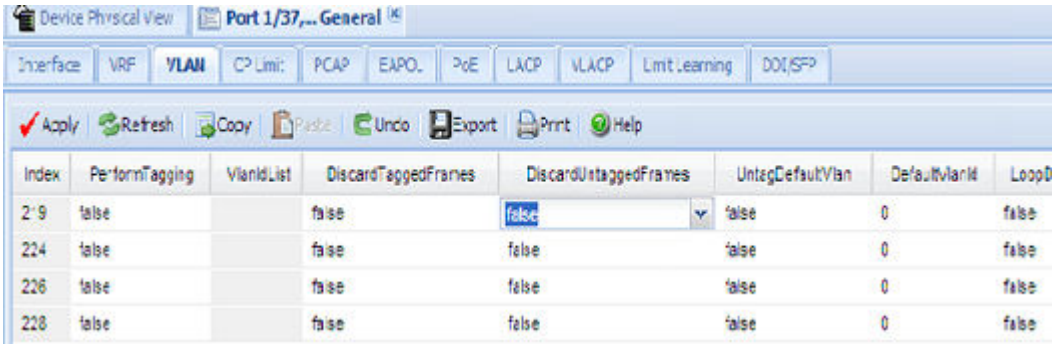
Note:

You can expand the appropriate folders for any feature you are configuring, and select a table-based tab.

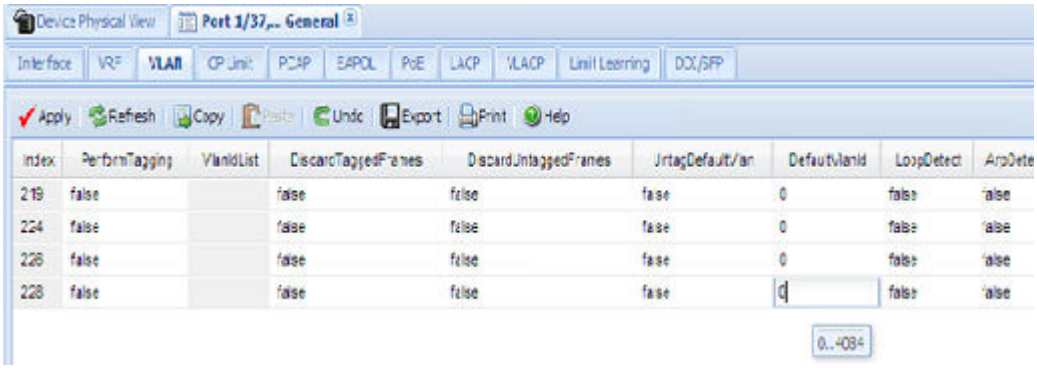
Procedure

1. In the Device Physical View, select multiple ports.
2. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port** > **General**.
3. Click the **VLAN** tab.

   The system displays a table-based tab with the VLAN information.
4. Click a table-based tab.
5. Double-click a white-shaded field to edit the value.
6. Click the arrow in the list field to view the options, and select the appropriate value.



7. In a text-entry field, double-click and edit the value.



8. Click **Apply** to save the configuration changes.

Monitoring multiple ports and configuration support

About this task

You can monitor or apply the same configuration changes to more than one port by using the multiple port selection function. You can use the standard menu or the shortcut menu to edit the configuration settings for multiple ports.

Tip:

A selected port shows a yellow outline around the port.

Procedure

1. Click the **Device Physical View** tab.
2. To select multiple ports, press the `Control` key, and click the required ports.

   Note:

   If you are using an embedded Enterprise Device Manager (EDM), you can select a maximum of 24 ports.

Opening folders and tabs

Use the following procedure to navigate in EDM.

Procedure

1. In the navigation pane, expand the **Configuration** folder.
2. Click the subfolder, for example, the **VLAN** folder.
3. In a folder or subfolder, click a tab to open that tab.

Undocking and docking tabs

About this task

Perform this procedure to undock a tab. You can undock tabs to have more than one tab visible at a time.

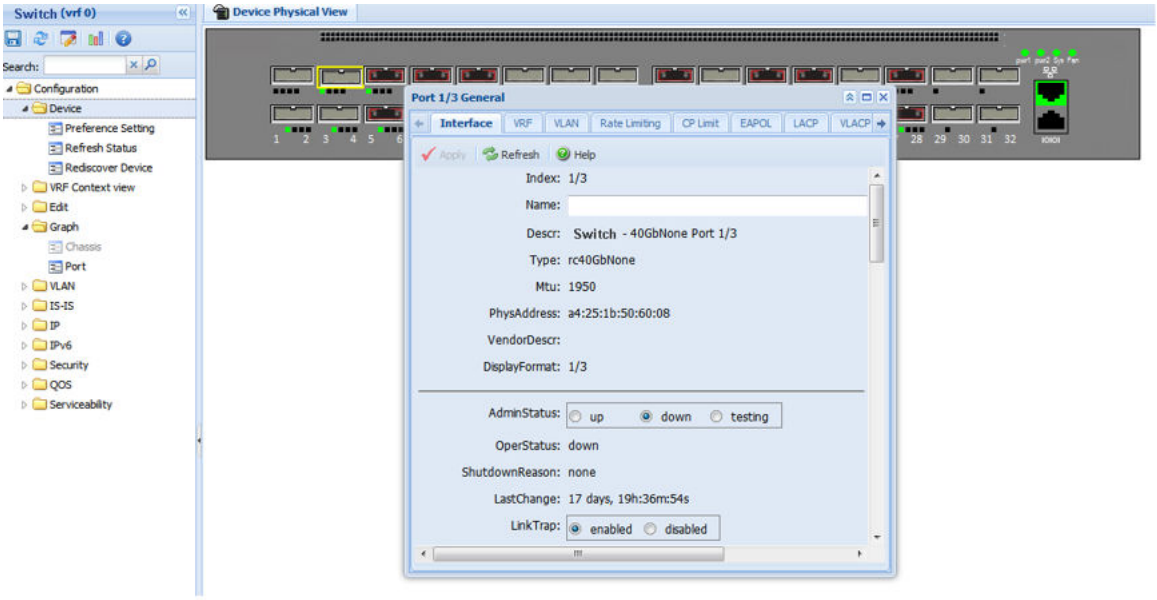
Procedure

1. In the navigation pane, click a tab.
2. In the menu bar, click and drag a tab to undock it.
3. In the upper-right corner of the tab, click **pages** to dock the tab.

Example of undocking and docking tabs

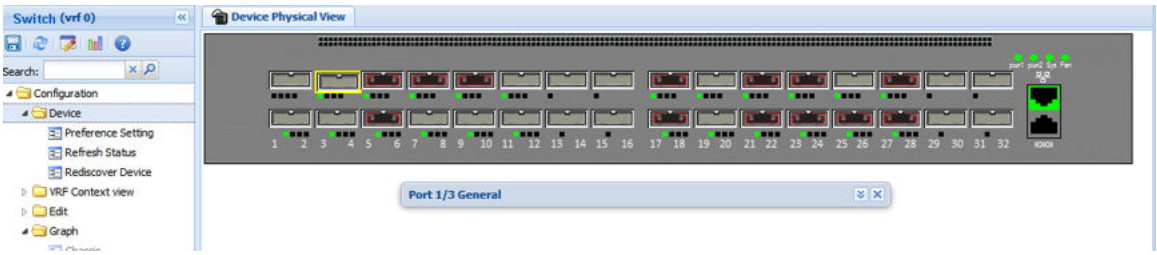
Procedure

1. Click the **Device Physical View** tab.
2. In the Device Physical View, select a port. In this example, right-click port 3.
3. In the Port shortcut menu, click **Edit General**.
4. Click and drag the Port 1/3 General tab wherever you want on the screen as shown in the following figure.



5. To reposition the tab anywhere on the screen, click and drag the title bar.
6. To manipulate the tab, click the buttons in the top-right of the dialog box.

7. Click the up arrowhead to minimize the tab. The minimized tab is shown in the following figure.



8. Click the down arrowhead button to restore the tab to its original size.

9. Click the pages button to dock the tab back into the menu bar.
10. Click the X button to close the tab.

Installing EDM help files

While the EDM GUI is bundled with the switch 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.

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

Procedure

1. On a TFTP or FTP server reachable from the switch, create a directory called **EDM_Help**.

   Ensure that you configure the switch with the host user name and password if you use FTP.
2. Unzip the EDM help zip file into the directory created in step 2.
3. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
4. Click **General**.
5. Click **Web**.
6. Enter the IP address of the file server and the path to the help files in the **HelpTFTPSourceDir** field, for example, 192.0.2.15:/home/Help/.

Chapter 6: File management in EDM

This chapter contains procedures for managing files with Enterprise Device Manager (EDM).

Use the File System tab to perform the following tasks:

- Copy a file.
- Check the amount of memory used and the number of files stored in the internal flash memory.
- Verify the name, size, and storage date of each file present in the internal flash memory.

Copying files

Use the following procedure to copy a file.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. In the **Source** field, specify the file you want to copy. Use one of the following options:
   - /intflash/<file>
   - /usb/<file>

     Note:

     The USB option does not apply to all hardware platforms.
   - x:x:x:x:x:x:x:x:<file>
   - <A.B.C.D>:<file>
4. In the **Destination** field, specify the file you want to copy. Use one of the following options:
   - /intflash/<file>
   - /usb/<file>

     Note:

     The USB option does not apply to all hardware platforms.
   - x:x:x:x:x:x:x:x:<file>
   - <A.B.C.D>:<file>

5. In the **Action** field, click **start**.
6. Click **Apply** to start copying the files.

   The system displays the results of the copy action in the Result field.

Viewing file storage information

Use the following procedure to view the file storage information for the switch.

About this task

This procedure displays the name of the storage, the number of bytes used, and the number of bytes free.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Storage Usage** tab.

Displaying internal flash files

Display information about the files on the internal flash.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Flash Files** tab.

Flash Files field descriptions

Use the data in the following table to use the **Flash Files** tab.

Name	Description
Slot	Specifies the slot number.
Name	Specifies the directory name of the flash file.
Date	Specifies the creation or modification date of the flash file.
Size	Specifies the size of the flash file.

Displaying USB file information

About this task

Display information about the files on a USB flash device to view general file information.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **USB Files** tab.

USB Files field descriptions

Use the data in the following table to use the **USB Files** tab.

Name	Description
Slot	Specifies the slot number.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

Glossary

command line interface (CLI)	A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Enterprise Device Manager (EDM)	A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
graphical user interface (GUI)	A graphical (rather than textual) computer interface.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.