BROCADE

COMMAND REFERENCE GUIDE

Network OS Command Reference, 5.0.2c

Supporting Network OS 5.0.2c

53-1004786-01
18 July 2016

© 2016, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, ClearLink, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier font`	Identifies CLI output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
	In Fibre Channel products, square brackets may be used instead for this purpose.

Convention	Description
x | y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS 5.0.1, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Network OS:

- Brocade VDX 2740 embedded switch
- Brocade VDX 6740
  - Brocade VDX 6740-48
  - Brocade VDX 6740-64
- Brocade VDX 6740T
  - Brocade VDX 6740T-48
  - Brocade VDX 6740T-64
  - Brocade VDX 6740T-1G
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

To obtain information about an OS version other than Network OS v5.0.1, refer to the documentation specific to that OS version.

What's new in this document

A listing of changes made since the Network OS Command Reference was last released.

New and modified commands

This document supports the enhancements introduced in Network OSv5.0.2.

The **copy** command has been updated to support TFTP.

The **snmp trap link-status** has been added to configure SNMP traps for interfaces.

For complete information, refer to the Network OS Release Notes.

New and modified commands

This document supports the enhancements introduced in Network OSv5.0.2a.

No command changes for this release.

For complete information, refer to the Network OS Release Notes.

New and modified commands

This document supports the enhancements introduced in Network OSv5.0.2b.

The **system tunnel suppress-debounce** command has been added to improve tunnel functionality.

For complete information, refer to the Network OS Release Notes.

New and modified commands

This document supports the enhancements introduced in Network OSv5.0.2c.

The **bp-rate-limit** command has been added.

For complete information, refer to the Network OS Release Notes.

Using the Network OS CLI

DCB command line interface

The Brocade Data Center Bridging (DCB) CLI is designed to support the management of DCB and Layer 2 Ethernet switching functionality. The Network OS CLI uses an industry-standard hierarchical shell familiar to Ethernet/IP networking administrators.

The system starts up with the default Network OS configuration and the DCB startup configuration. After logging in, you are in the Network OS shell. For information on accessing the DCB commands from the Network OS shell, refer to Network OS CLI command modes on page 38.

Saving your configuration changes

Any configuration changes made to the switch are written into the *running-config* file. This is a dynamic file that is lost when the switch reboots. During the boot sequence, the switch resets all configuration settings to the values in the *startup-config* file.

To make your changes permanent, use the **copy** command to commit the *running-config* file to the *startup-config* file, as shown below.

The following example illustrates the use of the **copy running-config** in privileged EXEC mode to save configuration changes:

```
switch# copy running-config startup-config
```

RBAC permissions

Role-Based Access Control (RBAC) defines the capabilities that a user account has based on the role the account has been assigned.

A role is an entity that defines the access privileges of the user accounts on the switch. A user is associated with one role. Refer to the *Network OS Administration Guide* for more information about RBAC.

Default roles

Attributes of default roles cannot be modified; however, the default roles can be assigned to non-default user accounts. The following roles are default roles:

- The admin role has the highest privileges. All CLIs are accessible to the user associated with the admin role. By default, the admin role has read and write access.
- The user role has limited privileges that are mostly restricted to show commands in privileged EXEC mode. User accounts associated with the user role cannot access configuration CLIs that are in global configuration mode. By default, the user role has read-only access.

Accessing the Network OS CLI through Telnet

NOTE
While this example uses the admin role to log in to the switch, both the admin and the user role can be used.

The procedure to access the Network OS CLI is the same through either the console interface or through a Telnet session; both access methods bring you to the login prompt.

```
switch login: admin
Password:**********
switch#
```

NOTE
Multiple users can open Telnet sessions and issue commands by using privileged EXEC mode. Network OS supports up to 32 Telnet sessions with the admin login.

Network OS CLI command modes

The following lists the major Network OS CLI command modes and describes how to access them.

NOTE
Use the **pwd** command to view the mode of the current working directory. This command function sin global configuration mode and the modes accessed from global configuration mode.

NOTE
Pressing Ctrl+Z or entering the end command in any mode returns you to privileged EXEC mode. Entering exit in any mode returns you to the previous mode.

TABLE 1 Network OS CLI command modes

Command mode	Prompt	How to access the command mode	Description
Privileged EXEC	`switch#`	This is the default mode for the switch.	Display and change system parameters. Note that this is the administrative mode and includes the basic configuration commands.
Global configuration	`switch(config)#`	From privileged EXEC mode, enter the **configure terminal** command.	Configure features that affect the entire switch.

TABLE 1 Network OS CLI command modes (continued)

Command mode	Prompt	How to access the command mode	Description

line vty	`switch(config)#line vty`
	`exec-timeout 60`
	`switch(config-line-vty)#`
		From global configuration mode, enter the **line vty** command.	Specify the amount of time a CLI session can be idle before it logs you out.

RBridge ID configuration mode	RBridge ID:
	`switch (config)# rbridge-id 1`
	`switch (config-rbridge-id-1)#`
		From global configuration mode, specify a node by entering the **rbridge-id** *rbridge_id* command, where *rbridge_id* is the RBridge ID of the selected node.	Configure features and issue show commands specific to an individual node in a Virtual Cluster Switching (VCS) environment. This includes both fabric cluster and management cluster scenarios.

Interface subtype	Port-channel:
	`switch(config-Port-channel-63)#`
	10-Gigabit Ethernet (DCB port):
	`switch(conf-if-te-0/1)#`
	VLAN: :
	`switch(config-Vlan-1)#`
	VE:
	`switch(config)# rbridge-id 11`
	`switch(config-rbridge-id-11)# int ve 56`
	`switch(config-Ve-56)#`
	Management
	`switch(config)# interface management 3/1`
	`switch(config-Management-3/1)`
		From global configuration mode, specify an interface by entering one of the following commands:
		• **interface fcoe**
		• **interface fortygigabitethernet**
		• **interface gigabitethernet**
		• **interface hundredgigabitethernet**
		• **interface loopback**
		• **interface management**
		• **interface port-channel**
		• **interface tengigabitethernet**
		• **interface ve**
		• **interface vlan**
			Access and configure individual interface subtypes.
			Enter **?** at a command prompt to see what interface subtypes are available for that command.

Protocol configuration	LLDP:
	`switch(conf-lldp)#`
	Spanning-tree:
	`switch(config-mstp)#`
	`switch(config-rstp)#`
	`switch(config-stp)#`
	`switch(config-pvst)#`
	`switch(config-rpvst)#`
	`switch(conf-udld)#`
		From global configuration mode, specify a protocol by entering one of the following commands:
		• **protocol lldp**
		• **protocol spanning-tree mstp**
		• **protocol spanning-tree rstp**
		• **protocol spanning-tree stp**
		• **protocol spanning-tree pvst**
		• **protocol spanning-tree rapid-pvst**
		• **protocol udld**
			Access and configure protocols.

FCoE configuration	FCoE:
	`switch(config-fcoe)#`
	FCoE fabric-map sub-mode:
	`switch(config-fcoe-fabric-map)#`
		From global configuration mode, use the **fcoe** command to enter FCoE configuration mode.
		From FCoE configuration mode, specify an FCoE sub-mode by entering one of the following commands:
		• **fabric-map default**
		• **map default**
			Access and configure FCoE features.

TABLE 1 Network OS CLI command modes (continued)

Command mode	Prompt	How to access the command mode	Description
	FCoE map sub-mode: `switch(config-fcoe-map)#`		

Access Gateway (AG)
configuration
	AG configuration mode:
	`switch(config-rbridge-12-ag)#`
	N_Port configuration mode:
	`switch(config-rbridge-12-ag-nport-if-fi- port )#`
	Port Grouping configuration mode:
	`switch(config-rbridge-12-ag-pg- pgid )#`
		From RBridge-ID configuration mode, enter the **ag** command.
		From AG configuration mode, enter the **nport** *port* command where port is an N_Port number supported by the hardware platform.
		From AG configuration mode, enter **pg** *pgid* where *pgid* is the port group identification number.
			Access and configure Access Gateway features.

AMPP port-profile mode	AMPP port-profile:
	`switch(config-port-profile-name)#`
	VLAN-profile sub-mode:
	`switch(config-vlan-profile)#`
	QoS-profile sub-mode:
	`switch(config-qos-profile)#`
	FCoE-profile sub-mode:
	`switch(config-fcoe-profile)#`
	Security-profile sub-mode:
	`switch(config-security-profile)#`
		From the global configuration mode, enter the **port-profile** command to enter port-profile configuration mode.
		From port-profile configuration mode, specify an AMPP sub-mode by entering one of the following commands:
		• **vlan-profile**
		• **qos-profile**
		• **fcoe-profile**
		• **security-profile**
			Access and configure AMPP features.

Routing protocol configuration	BGP:
	`switch(config)#`
	`switch(config-rbridge-id-1)#`
	`switch(config-bgp-router)#`
	BGP route-map configuration mode:
	`switch(config-rbridge-id-1)#`
	`switch(config-route-map-myroutemap/permit/1)#`
	BGP address-family IPv4-unicast mode:
	`switch(config-bgp-router)#`
	`switch(config-bgp-ipv4u)#`
		From global configuration mode, specify an RBridge ID to enter RBridge ID configuration mode.
		From RBridge ID configuration mode, use the **router bgp** command to enter BGP configuration mode.
		From RBridge ID configuration mode, use the **route-map** command with a **permit** or **deny** statement and an instance number to enter BGP route-map configuration mode,.
		From BGP configuration mode, use the **address-family ipv4 unicast** command to enter BGP address-family IPv4 unicast configuration mode.
			Configure Border Gateway Protocol routing protocol

TABLE 1 Network OS CLI command modes (continued)

Command mode	Prompt	How to access the command mode	Description

	OSPF VRF:
	`switch(config)# rbridge-id 5`
	`switch(config-rbridge-id-5)# router ospf`
	`switch(config-router-ospf-vrf-default-vrf)#`
		From RBridge ID configuration mode, use the **router ospf** command to enter OSPF VRF configuration mode.	Configure Open Short Path First routing protocol

	PIM:
	`switch(config)# rbridge-id 5`
	`switch(config-rbridge-id-5)# router pim`
	`switch(conf-pim-router)#`
		From Bridge ID configuration mode, use the **router pim** command to enter PIM configuration mode.	Configure Protocol Independent Multicast routing protocol

Virtual-router-group configuration mode	`switch(config)# rbridge-id 101`
	`switch(config-rbridge-id-101)# int ve 25`
	`switch(config-ve-25)# vrrp-extended-group 1`
	`switch(config-vrrp-extended-group-1)#`
		From RBridge ID configuration mode, use the **int ve** command to enter VE configuration mode. Then use the **vrrp-extended-group** command to enter virtual-router-group configuration mode.	

ACL configuration mode	Standard ACL:
	`switch(config-macl-std)#`
	`switch(config-ipacl-std)#`
	`switch(config-ip6acl-std)#`
	Extended ACL:
	`switch(config-macl-ext)#`
	`switch(config-ipacl-ext)#`
	`switch(config-ip6acl-ext)#`
		From global configuration mode, enter one of the following commands:
		• **mac access-list standard**
		• **mac access-list extended**
		• **ip access-list standard**
		• **ip access-list extended**
		• **ipv6 access-list standard**
		• **ipv6 access-list extended**
			Access ACL configuration mode to manage access control lists (ACLs) .

CEE map configuration mode	CEE map: `switch(config-cee-map-default)#`	From global configuration mode, enter the **cee-map default** command.	Access and configure CEE map features.
ELD configuration mode	`switch(config)# protocol edge-loop-detection` `switch(config-eld)#`	From global configuration mode, enter the **protocol edge-loop-detection** command.	Configure edge loop detection.
Hardware configuration	`switch(config)# hardware`	From global configuration mode, specify the hardware mode by entering the **hardware** command.	This mode is a prerequisite for entering connector and port-group mode.
Connector mode	`switch# hardware connector` `switch(config-connector [n]/n/n)#`	From hardware mode, specify the connector node and [*rbridge-id*]/*slot*/*port* information.	Connector mode is used to enable breakout on ports. When breakout is enabled, ports are appended in the output with a colon(:) followed by values 1-4.
DSCP mutation mapping	DSCP Mutation Map: `switch(dscp-mutation-mapname)#`	From global configuration mode, remap incoming DSCP values by entering the **qos map dscp-mutation** *mapname*command:	

TABLE 1 Network OS CLI command modes (continued)

Command mode	Prompt	How to access the command mode	Description
DSCP to CoS priority mapping	DSCP to CoS Map: `switch(dscp-cos-mapname)#`	From global configuration mode, create a DSCP to CoS priority map by entering the **qos map dscp-cos** *mapname* command.	
DSCP to traffic class mapping	DSCP to Traffic Class Map: `switch(dscp-traffic-class-mapname)#`	From global configuration mode, create a DSCP to traffic class map by entering the **qos map dscp-traffic-class** *mapname* command:	
Port-group configuration	`switch(config-port-group-1/3/9)#`	From hardware configuration mode, enter the **port-group** command followed by a port group identification: p**ort-group** *rbridge-id/slot/port-group-id* The port-group-id is specific to the Brocade VDX 8770 switch 27x40 GbE line card.	This mode allows you to enable Performance or Density operating modes on a specific port group on the 27x40 GbE line card only.

QoS Policer configuration	Police Priority Map
	`switch(config-policemap)#`
	Class Map:
	`switch(config-classmap)#`
	Policy Map:
	`switch(config-policymap)#`
	Policy-class-map submode:
	`switch(config-policymap-class)#`
	Policy-class-map-policer attributes submode:
	`switch(config-policymap-class-police)#`
		From global configuration mode, specify a Policer configuration mode by entering one of these command:
		• **police-priority-map** *mapname*
		• **class-map** *mapname*
		• **policy-map** *mapname*
		To enter the policy-class-map sub-mode from policy-map mode, enter **class** *classmapname*
		To enter the policy-class-map-policer attributes sub-mode from policy-map-class mode, enter **police** followed by the policing attributes.	

Alias configuration	`switch(config-alias-config)#`	From global configuration mode, enter the **alias-config** command. Use the **alias** *string* expansion command to create aliases.	Access configure alias features.
User alias configuration	`switch(config-alias-config-user)#`	From alias configuration mode, enter the **user** *name*command.	Access configure user alias features.
Policymap configuration	`switch(config-policymap)#`	From global configuration mode, enter the **policy-map** *name* command.	
Policymap class map configuration	`switch(config-policymap-class)#`	From policymap configuration mode, enter the **class** *name*command.	
Policymap class police configuration	`switch(config-policymap-class-police)#`	From policymap class configuration mode, enter the **police cir** *value* command.	
VCS configuration mode	`switch(config-vcs)#`	From privileged EXEC mode, enter the **vcs vcsid** *id-number* **logical-chassis enable** command	

TABLE 1 Network OS CLI command modes (continued)

Command mode	Prompt	How to access the command mode	Description
VRF configuration mode	`(config-rbridge-12-vrf-vrf_name)#`	From RBridge ID configuration mode, enter the **vrf** *name* command.	

Network OS CLI keyboard shortcuts

The following lists Network OS CLI keyboard shortcuts.

TABLE 2 Network OS CLI keyboard shortcuts

Keystroke	Description
Ctrl+B (or the left arrow key)	Moves the cursor back one character.
Ctrl+F (or the right arrow key)	Moves the cursor forward one character.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl+Z	Returns to privileged EXEC mode.
Ctrl+P (or the up arrow key)	Displays commands in the history buffer with the most recent command displayed first.
Ctrl+N (or the down arrow key)	Displays commands in the history buffer with the most recent command displayed last.

NOTE

In privileged EXEC mode, use the **show history** command to list the commands most recently entered. The switch retains the history of the last 1000 commands entered for the current session.

Using the do command as a shortcut

You can use the **do** command to save time when you are working in any configuration mode and you want to run a command in privileged EXEC mode.

For example, if you are configuring LLDP and you want to execute a privileged EXEC mode command, such as the **dir** command, you would first have to exit the LLDP configuration mode. By using the **do** command with the **dir** command, you can ignore the need to change configuration modes, as shown in the following example.

```
switch(conf-lldp)# do dir
Contents of flash://
  -rw-r-----      1276  Wed Feb 4 07:08:49 2009  startup_rmon_config
  -rw-r-----      1276  Wed Feb 4 07:10:30 2009  rmon_config
  -rw-r-----      1276  Wed Feb 4 07:12:33 2009  rmon_configuration
  -rw-r-----      1276  Wed Feb 4 10:48:59 2009  startup-config
```

Displaying Network OS CLI commands and command syntax

Enter a question mark (?) in any command mode to display the list of commands available in that mode.

```
switch(conf-lldp)# ?
Possible completions:
 advertise           The Advertise TLV configuration.
 description         The User description
 disable             Disable LLDP
 do                  Run an operational-mode command
 exit                Exit from current mode
 hello               The Hello Transmit interval.
 help                Provide help information
 iscsi-priority      Configure the Ethernet priority to advertise for iSCSI
 mode                The LLDP mode.
 multiplier          The Timeout Multiplier
 no                  Negate a command or set its defaults
 profile             The LLDP Profile table.
 pwd                 Display current mode path
 system-description  The System Description.
 system-name         The System Name
 top                 Exit to top level and optionally run command
```

To display a list of commands that start with the same characters, type the characters followed by the question mark (**?**).

```
switch# e?
Possible completions:
 exit  Exit the management session
```

To display the keywords and arguments associated with a command, enter the keyword followed by the question mark (?).

```
switch# terminal ?
Possible completions:
 length    Sets Terminal Length for this session
 monitor   Enables terminal monitoring for this session
 no        Sets Terminal Length for this session to default :24.
 timeout   Sets the interval that the EXEC command interpreter wait for user input.
```

If the question mark (?) is typed within an incomplete keyword, and the keyword is the only keyword starting with those characters, the CLI displays help for that keyword only.

```
switch# show d?
Possible completions:
 debug  Debug
 diag   Show diag related information
 dot1x  802.1x configuration
 dpod   Provides DPOD license information.
```

If the question mark (?) is typed within an incomplete keyword but the keyword matches several keywords, the CLI displays help for all the matching keywords.

```
switch# show i?
 interface Interface status and configuration
 ip     Internet Protocol (IP)
```

The Network OS CLI accepts abbreviations for commands. This example is the abbreviation for the **show qos interface all** command.

```
switch# sh q i a
```

If the switch does not recognize a command after **Enter** is pressed, an error message displays.

```
switch# hookup
                ^
syntax error: unknown argument.
```

If an incomplete command is entered, an error message displays.

```
switch# show
                    ^
syntax error: unknown argument.
```

Completing Network OS CLI commands

To complete the spelling of commands or keywords automatically, begin typing the command or keyword and then press **Tab**. For example, at the CLI command prompt, type `te` and press **Tab**:

```
switch# te
```

The CLI displays the following command.

```
switch# terminal
```

If there is more than one command or keyword associated with the characters typed, the Network OS CLI displays all choices. For example, at the CLI command prompt, type `show l` and press **Tab**.

```
switch# show l
```

The CLI displays the following command.

```
Possible completions:
 lacp     LACP commands
 license  Display license keys installed on the switch.
 lldp     Link Layer Discovery Protocol(LLDP).
 logging  Show logging
```

Using Network OS CLI command output modifiers

You can filter the output of the Network OS CLI **show** commands by using the output modifiers described below.

TABLE 3 Network OS CLI command output modifiers

Output modifier	Description
append	Appends the output to a file.
redirect	Redirects the command output to the specified file.
include	Displays the command output that includes the specified expression.
exclude	Displays the command output that excludes the specified expression.
begin	Displays the command output that begins with the specified expression.
last	Displays only the last few lines of the command output.
tee	Redirects the command output to the specified file. Notice that this modifier also displays the command output.
until *string*	Ends the output when the output text matches the string.
count	Counts the number of lines in the output.
linnum	Enumerates the lines in the output.
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Considerations for show command output

Network OS contains many versions of the **show** command. The output of the **show** command changes depending on your configuration and situation. However, in general terms the **show** command falls into one of two categories:

- Any **show** commands that are fabric (global configuration) in nature, such as VLAN, MAC Address table, AMPP, Zoning, and so on, should display or clear the information for all nodes in a logical chassis.
- Any **show** commands that are local to a switch, such as Layer 3 or Layer 2 functionality (for example, sFlow, SPAN, and so on), should display the local information by default, and display different switch information specific to an RBridge ID.

User-configurable VLAN IDs

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). VLAN 1002 is reserved for FCoE VLAN functionality on all VDX switches. Valid VLAN IDs (those configurable by the user), as well as VLAN IDs reserved for system functionality, are shown in the following table.

TABLE 4 User-configurable and reserved VLAN IDs for Brocade VDX 8770 series, VDX 6740 series, and VDX 2740 switches

802.1Q VLANs	Classified VLANs (for Virtual Fabrics)
VLAN IDs 1 through 4086 (VLAN IDs 4087 through 4095 are reserved on these switches)	VLAN IDs 4096 through 8191 for service or transport VFs in a Virtual Fabrics context

Commands A through E

aaa authentication

Configures the AAA login sequence.

Syntax

aaa authentication login { **default** | **ldap** | **local** | **radius** { **local** | **local-auth-failback** } | **tacacs+** { **local** | **local-auth-failback** } }

no aaa authentication login

Command Default

The default server is Local.

Parameters

login

Specifies the type of server that will be used for authentication, authorization, and accounting (AAA) on the switch. The local server is the default. Specify one of the following options:

default

Specifies the default mode (local server). Authenticates the user against the local database only. If the password does not match or the user is not defined, the login fails.

ldap

Specifies the Lightweight Directory Access Protocol (LDAP) servers.

local

Specifies to use the local switch database if prior authentication methods are inactive.

local-auth-failback

Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

local

Specifies the local switch database.

radius

Specifies the RADIUS servers.

local

Specifies to use the local switch database if prior authentication methods are inactive.

local-auth-failback

Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

tacacs+

Specifies the TACACS+ servers.

local
Specifies to use the local switch database if prior authentication methods are inactive.

local-auth-failback
Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

Modes

Global configuration mode

Usage Guidelines

This command selects the order of authentication sources to be used for user authentication during the login process. Two sources are supported: primary and secondary. The secondary source of authentication is optional and will be used if the primary source fails or is not available.

The authentication mode can only be set and cannot be added or deleted. For example, to change a configuration from "radius local" to radius only, execute the **no aaa authentication login** command to resets the configuration to the default mode, and then reconfigure the AAA mode with the desired setting.

In a configuration with primary and secondary sources of authentication, the primary mode cannot be modified alone. For example, you cannot change from “radius local" or "radius local-auth-fallback” to “tacacs+ local" or "tacacs+ local-auth-fallback” respectively. First remove the existing configuration and then configure it to the required configuration.

Beginning with Network OS v4.0.0, when the local option is specified as a secondary authentication service, local authentication is tried only when the primary AAA authentication service (TACACS+/Radius/LDAP) is either unreachable or not available. Local authentication will not be attempted if the authentication with the primary service fails.

Examples

To change the AAA server to TACACS+ using the local switch database as a secondary source of authentication:

```
switch(config)# aaa authentication login tacacs+ local
Broadcast message from root (pts/0) Tue Apr  5 16:34:12 2011...
```

To change the AAA server from TACACS+ and local to TACACS+ only (no secondary source):

```
switch(config)# no aaa authentication login tacacs+ local
switch(config)# aaa authentication login tacacs+
switch(config)# do show running-config aaa
aaa authentication login tacacs+
```

Related Commands

show running-config aaa

accept-unicast-arp-request

Configures the IPv4 fabric-virtual-gateway active sessions to respond to unicast ARP requests.

Syntax

accept-unicast-arp-request

no accept-unicast-arp-request

Modes

IPv4 address-family configuration mode

Usage Guidelines

The **no accept-unicast-arp-request** command configures the active sessions to ignore ARP requests.

This command functions for IPv4 traffic only.

Examples

The following example shows how to configure the gateway MAC address for an IPv4 Fabric-Virtual-Gateway session to respond to unicast ARP requests.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv4
switch(conf-address-family-ipv4)# accept-unicast-arp-request
```

History

Release version	Command history
5.0.1	This command was introduced.

access-group

Applies rules specified in an access control list (ACL) to traffic entering or exiting an interface. You can use the **no** form of this command to remove an ACL from an interface.

Syntax

{ **ip**| **ipv6** | **mac** } **access-group** *ACLname* { **in** | **out** }

no { **ip**| **ipv6** | **mac** } **access-group** *ACLname* { **in** | **out** }

Parameters

ip
: Specifies the Layer 2 or Layer 3 ACL to bind to an interface.

ipv6
: Specifies the Layer 2 or Layer 3 ACL to bind to an interface.

mac
: Specifies the Layer 2 or Layer 3 ACL to bind to an interface.

in
: Specifies the ACL binding direction as ingress.

out
: Specifies the ACL binding direction as egress.

ACLname
: Specifies the ACL name.

Modes

Interface subtype configuration mode

Usage Guidelines

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL
- One egress MAC ACL
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL
- One egress IPv6 ACL

NOTE
You can apply an ACL to multiple interfaces. And you can apply an extended ACL twice—ingress and egress—to a given user interface.

To remove an IPv4 ACL from an interface, enter the **no** form of this command.

Examples

```
switch# configure
Entering configuration mode terminal
switch(config)# int ten 122/5/34
switch(conf-if-te-122/5/34)# ip access-group ag1 in
```

access-list

Creates a standard or extended access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

{ **ip**| **ipv6** | **mac** } **access-list** { **standard** | **extended** } *ACLname*

no { **ip**| **ipv6** | **mac** } **access-list** { **standard** | **extended** } *ACLname*

Parameters

ip
: Specifies the Layer 2 or Layer 3 ACL type.

ipv6
: Specifies the Layer 2 or Layer 3 ACL type.

mac
: Specifies the Layer 2 or Layer 3 ACL type.

standard
: Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended
: Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters.

ACLname
: Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

On any given switch, an ACL name must be unique among all ACL types (MAC/IPv4/IPv6; standard or extended).

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after if is applied to an interface, using the **access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates a standard IPv6 ACL:

```
switch # configure
switch(config)# ipv6 access-list standard stdV6ACL1
```

The following example creates an extended IPv6 ACL:

```
switch # configure
switch(config)# ipv6 access-list extended extdACL5
```

activate (NSX Controller connection profile)

Activates an NSX controller connection profile, thereby initiating the connection between the NSX controller and the VCS fabric.

Syntax

activate

no activate

Command Default

Profile is inactive.

Modes

NSX Controller configuration mode

Usage Guidelines

This command is allowed for a switch that is in logical chassis cluster mode only.

You must configure the NSX Controller IP address before executing this command.

You must configure the VCS virtual IP address of the cluster before executing this command.

Use the **no** form of the command to mark the connection profile inactive. Any existing connection is closed. However, all tunnels already created by the NSX controller remain open.

Examples

To activate an NSX controller connection profile that you have created and named profile1:

```
switch# configuration
switch(config)# nsx-controller profile1
switch(config-nsx-controller-profile1)# activate
```

activate (protected VLAG)

Activates the port-channel redundancy group.

Syntax

activate

no activate

Modes

Global configuration mode

Usage Guidelines

Use this command to activate the port-channel redundancy group to activate the protected VLAG. Once activated, no configuration changes are allowed on the protected VLAG and members.

The **no activate** command deactivates the protected VLAG.

Examples

Typical command execution example:

```
switch(config-port-channel-redundancy-group-32)# activate
```

Related Commands

port-channel, port-channel-redundancy-group

activate (VXLAN gateway)

Activates a VXLAN overlay gateway instance.

Syntax

activate

no activate

Command Default

By default, a gateway is not activated during initial configuration.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

It is recommended that you configure all gateway parameters before activating the gateway. This operation enables all tunnels that are associated with this gateway. VXLAN tunnels are not user configurable.

The following conditions that must be in place before you can execute the **activate** command:

- Loopback interfaces must be configured on all RBridges that have been attached by means of the **attach** command. Refer to the **interface loopback** command,
- All loopback interfaces must be configured with the same IPv4 address and the same VRF instance.
- The IP address of the VXLAN gateway must be configured. Refer to the **ip interface** command.
- If attached RBridges are configured for a VXLAN gateway, the VE, VRID and VRF configurations must match on all attached RBridges.

Use the **no activate** command in VXLAN overlay gateway configuration mode to deactivate the gateway. All associated tunnels are also deactivated.

Examples

The following example activates a VXLAN gateway named "gateway1" . The gateway was previously configuredby means of the **overlay-gateway** command:

```
switch# configure terminal
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# activate
```

Related Commands

attach vlan, interface loopback, ip interface, overlay-gateway

address-family (BGP)

Enables the IPv4 or IPv6 address-family configuration mode to configure a variety of BGP4 unicast routing options.

Syntax

address-family { **ipv4** | **ipv6** } **unicast**

no address-family { **ipv4** | **ipv6** } **unicast**

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove IPv4 or IPv6 address-family configurations from the device.

Examples

To enable BGP IPv4 address-family configuration mode:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)#
```

To enable BGP IPv6 address-family configuration mode:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)#
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

address-family (Fabric-Virtual-Gateway)

Enables IPv4 or IPv6 address family for the Fabric-Virtual-Gateway at VCS global level.

Syntax

address-family { **ipv4** | **ipv6** }

no address-family { **ipv4** | **ipv6** }

Command Default

Both IPv4 and IPv6 address families are enabled when global router Fabric-Virtual-Gateway configuration is created.

Parameters

ipv4

Enables IPv4 address family.

ipv6

Enables IPv6 address family.

Modes

Router Fabric-Virtual-Gateway configuration mode

Usage Guidelines

Use the **no** form of the command to disable the specific IPv4 or IPv6 address family.

Examples

The following example shows how to configure the IPv4 address family for the Fabric-Virtual-Gateway.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv4
```

The following example shows how to configure the IPv6 address family for the Fabric-Virtual-Gateway.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv6
```

History

Release version	Command history
5.0.1	This command was introduced.

address-family (VRF)

Enables the IPv4 or IPv6 address-family configuration mode to configure a variety of VRF unicast routing options.

Syntax

address-family { **ipv4** | **ipv6** } **unicast**

no address-family { **ipv4** | **ipv6** } **unicast**

Modes

VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove IPv4 or IPv6 address-family configurations from the device.

Examples

To enable IPv4 address-family configuration mode for VRF routing:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# vrf orange
switch(config-vrf-orange)# address-family ipv4 unicast
switch(config-ipv4-unicast)#
```

To enable IPv6 address-family configuration mode for VRF routing:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# vrf red
switch(config-vrf-red)# address-family ipv6 unicast
switch(config-ipv6-unicast)#
```

advertise dcbx-fcoe-app-tlv

Advertises application Type, Length, Values (TLVs) to ensure interoperability of traffic over the Data Center Bridging eXchange protocol (DCBX), which runs over LLDP to negotiate an FCoE application TLV.

Syntax

advertise dcbx-fcoe-app-tlv

no advertise dcbx-fcoe-app-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Converged Enhanced Ethernet (CEE) parameters related to FCoE must be negotiated before FCoE traffic can begin on a CEE link. An FCoE application TLV is exchanged over LLDP, which negotiates information such as FCoE priority, and Priority Flow Control (PFC) pause.

Enter **no advertise dcbx-fcoe-app-tlv** to return to the default setting.

Related Commands

advertise dot1-tlv, advertise dot3-tlv, advertise optional-tlv

advertise dcbx-fcoe-logical-link-tlv

Advertises to any attached device the FCoE status of the logical link.

Syntax

advertise dcbx-fcoe-logical-link-tlv

no advertise dcbx-fcoe-logical-link-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no advertise dcbx-fcoe-logical-link-tlv** to return to the default setting.

Related Commands

advertise dcbx-fcoe-app-tlv

advertise dcbx-iscsi-app-tlv

Advertises the iSCSI traffic configuration parameters for Type, Length, Values (TLV) values.

Syntax

advertise dcbx-iscsi-app-tlv

no advertise dcbx-iscsi-app-tlv

Command Default

Advertisement is enabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

No verification or enforcement of the usage of the advertised parameters by the iSCSI server or target is done by the switch.

Enter **no advertise dcbx-iscsi-app-tlv** to return to the default setting.

Related Commands

advertise dcbx-fcoe-app-tlv

advertise dcbx-tlv

Advertises to any attached device mandatory Data Center Bridging eXchange protocol (DCBX) Type, Length, Values (TLV) values.

Syntax

advertise dcbx-tlv

no advertise dcbx-tlv

Command Default

Advertisement is enabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no advertise dcbx-tlv** to return to the default setting.

Related Commands

advertise dot1-tlv, advertise dot3-tlv, advertise optional-tlv

advertise dot1-tlv

Advertises to any attached device IEEE 802.1 organizationally specific Type, Length, Values (TLV) values.

Syntax

advertise dot1-tlv

no advertise dot1-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no advertise dot1-tlv** to return to the default setting.

Related Commands

advertise dcbx-tlv, advertise dot3-tlv, advertise optional-tlv

advertise dot3-tlv

Advertises to any attached device IEEE 802.3 organizationally specific Type, Length, Values (TLV) values.

Syntax

advertise dot3-tlv

no advertise dot3-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no advertise dot3-tlv** to return to the default setting.

Related Commands

advertise dcbx-tlv, advertise dot1-tlv, advertise optional-tlv

advertise optional-tlv

Advertises the optional Type, Length, and Values (TLV) values.

Syntax

advertise optional-tlv { **management-address** | **port-description** | **system-capabilities** | **system-description** | **system-name** }

no advertise optional-tlv

Command Default

Advertisement is disabled.

Parameters

management-address
Advertises the management address of the system.

port-description
Advertises the user-configured port.

system-capabilities
Advertises the capabilities of the system.

system-description
Advertises the system firmware version and the current image running on the system.

system-name
Advertises the name of the system.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no advertise optional-tlv** to return to the default setting.

Related Commands

advertise dcbx-tlv, advertise dot1-tlv, advertise dot3-tlv

advertise-backup

Enables a backup VRRP router to send advertisement frames to the master VRRP router.

Syntax

advertise-backup

no advertise backup

Command Default

Advertisement is disabled.

Modes

Virtual-router-group configuration mode

Usage Guidelines

If a backup router is enabled to send advertisement frames, the frames are sent every 60 seconds.

This command can be used for VRRP-E, but not for VRRP.

Enter **no advertise backup** to return to the default setting (no periodic transmission).

Examples

To enable the backup VRRP routers to send advertisement frames to the master VRRP router:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-extended-group 1
switch(config-vrrp-extended-group-1)# advertise-backup
```

Related Commands

advertisement-interval (VRRP), backup-advertisement-interval, vrrp-extended-group

advertisement interval (fabric-map)

Configures the FIP advertisement interval for the FCoE fabric-map mode.

Syntax

advertisement interval *milliseconds*

no advertisement interval

Command Default

8000 milliseconds

Parameters

milliseconds

The interval value in milliseconds. Valid values range from 250 through 90000 milliseconds.

Modes

FCoE fabric-map configuration mode

Usage Guidelines

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Enter **no advertisement interval** return to the default setting.

Examples

```
switch(config)# fcoe

switch(config-fcoe)# fabric-map default

switch(config-fcoe-fabric-map)# advertisement interval 8000
```

Related Commands

fcoe

advertisement-interval (VRRP)

Configures the interval at which the master VRRP router advertises its existence to the backup routers.

Syntax

advertisement-interval *range*

Command Default

1 second for version 2, 1000 milliseconds for version 3.

Parameters

range

Interval at which the master VRRP router advertises its existence to the backup routers. Valid values range from 1 through 255 seconds for VRRPv2 and from 100 through 40900 milliseconds for VRRPv3.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This interval is the length of time, in seconds, between each advertisement sent from the master to its backup VRRP routers. The advertisement notifies the backup routers that the master is still active. If the backup routers do not receive an advertisement from the master in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E and for VRRPv3 and VRRP-Ev3.

Examples

To set the advertisement interval to 30 seconds for VRRP-E group 10:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-extended-group 10
switch(config-vrrp-extended-group-10)# advertisement-interval 30
```

To set the advertisement interval to 3000 milliseconds for VRRP-Ev3 group 19:

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# interface ve 2019
switch(config-ve-2019)# ipv6 vrrp-extended-group 19
switch(config-vrrp-extended-group-19)# advertisement-interval 3000
```

Related Commands

backup-advertisement-interval, vrrp-extended-group, vrrp-group

advertisement-interval-scale

Configures subsecond intervals at which the master VRRP-Ev3 device advertises its existence to the backup routers.

Syntax

advertisement-interval-scale *scale*

Command Default

1

Parameters

scale

Number representing the scale of the division of a configured interval at which the master VRRP-Ev3 device advertises its existence to the backup devices. Valid values are 1, 2, 5 and 10.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command scales the advertisement interval of the master VRRP-Ev3 device as configured by the **advertisement-interval** command. A value of 1, 2, 5, or 10 can be set and the existing advertisement interval value is divided by the scaling value, for example, if the advertisement interval is set to 1 second and the scaling value is set to 10, the new advertisement interval is 100 milliseconds. When all the advertisement intervals in a VRRP-Ev3 session are scaled, subsecond VRRP-Ev3 convergence is possible if a master fails. The advertisement notifies the backup devices that the master is still active. If the backup devices do not receive an advertisement from the master in a designated amount of time, the backup device with the highest priority can assume the role of master. Using subsecond advertising intervals, subsecond device redundancy can be achieved.

This command is only supported by VRRP-Ev3.

Examples

To set the scaling of the advertisement interval to 500 milliseconds for VRRP-Ev3 group 19:

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# interface ve 2019
switch(config-ve-25)# ipv6 vrrp-extended-group 19
switch(config-vrrp-extended-group-10)# advertisement-interval 1
switch(config-vrrp-extended-group-10)# advertisement-interval-scale 2
```

Related Commands

advertisement-interval (VRRP)

ag

Enables Access Gateway (AG) configuration mode.

Syntax

ag

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command while in RBridge ID configuration mode for a specific RBridge ID. This command enables Access Gateway (AG) configuration mode on a specific switch. In this mode, you can configure Access Gateway features such as Access Gateway policies, VF_Port to N_Port mapping, Port Grouping, N_Port Monitoring reliability counters, and Modified Managed Fabric Name Monitoring (N-MFNM) mode timeout values.

Examples

Enabling AG configuration mode while in RBridge ID configuration mode.

```
sw0(config-rbridge-id-2)# ag
sw0(config-rbridge-id-2-ag)#
```

Related Commands

show ag, clear ag nport-utilization

ag enable

Enables Access Gateway mode on a switch as follows: Enables FC ports, configures them as N_Ports, and then maps them to VF_Ports.

Syntax

ag enable

no ag enable

Modes

Privileged EXEC mode

Usage Guidelines

Enabling Access Gateway mode reboots the switch.

The initial mapping of N_Ports to VF_Ports implements the current default mapping configuration.

To disable Access Gateway mode, enter the **no ag enable** command.

Examples

The following example enables AG mode on a local switch:

```
switch# ag enable
```

The following example disables AG mode on a local switch:

```
switch# no ag enable
```

History

Release version	Command history
5.0.0	The **rbridge-id** and **vcs-id** parameters are no longer supported for this command.

Related Commands

show ag, show ag map, show ag nport-utilization, show ag pg

aggregate-address (BGP)

Configures the device to aggregate routes from a range of networks into a single network prefix.

Syntax

aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

no aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Command Default

The address aggregation feature is disabled. By default, the device advertises individual routes for all networks.

Parameters

ip-addr
IPv4 address.

ip-mask
IPv4 mask.

ipv6-addr
IPv6 address.

ipv6-mask
IPv6 mask.

advertise-map
Causes the device to advertise the more-specific routes in the specified route map.

map-name
Specifies a route map to be consulted.

as-set
Causes the device to aggregate AS-path information for all routes in the aggregate routes from a range of networks into a single network prefix.

attribute-map
Causes the device to set attributes for the aggregate routes according to the specified route map.

summary-only
Prevents the device from advertising more-specific routes contained within the aggregate route.

suppress-map
Prevents the more-specific routes contained in the specified route map from being advertised.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the defaults.

Examples

To aggregate routes from a range of networks into a single network prefix and prevent the device from advertising more-specific routes:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# aggregate-address 10.11.12.0 summary-only
```

To aggregate routes from a range of networks into a single network prefix under the IPv6 address family and advertise the paths for this route as AS_SET:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# aggregate-address 2001:DB8:12D:1300::/64 as-set
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

alias

Configures the global or user-level alias for switch commands.

Syntax

alias *string expansion*

no alias *string expansion*

Parameters

string

Alias name string. The number of characters can be from 1 through 64.

expansion

Commands for the alias name. Multiple commands can be separated with a semicolon (;).

Modes

Alias configuration mode

User-alias configuration mode

Usage Guidelines

The global alias is visible to all users. When the global alias name is called, the configured alias expansion commands are executed on the prompt.

The user-level alias is accessible only when the respective user logs in.

Use the **no** form of his command to remove the alias. You must be in the correct configuration mode in order to remove the global or user alias.

Examples

The following example sets both a switch alias and a user alias.

```
switch(config)# alias-config
switch(config-alias-config)# alias user-alias "show clock"
switch(config-alias-config)# alias company Brocade
switch(config-alias-config)# alias redwood engineering
switch(config-alias-config)# user john smith
switch(config-alias-config-user)# alias manager engineering
```

Related Commands

alias-config, user (alias configuration)

alias-config

Launches the alias configuration mode, allowing you to configure the switch alias.

Syntax

alias-config

Modes

Global configuration mode

Examples

Example of setting a switch alias and a user alias.

```
switch(config)# alias-config
switch(config-alias-config)# alias user-alias "show clock"
switch(config-alias-config)# alias company Brocade
switch(config-alias-config)# alias redwood engineering
switch(config-alias-config)# user john smith
switch(config-alias-config-user)# alias manager engineering
```

Related Commands

alias, user (alias configuration)

allow non-profiled-macs

Specifies whether non-profiled MAC addresses on the profiled port are dropped.

Syntax

allow non-profiled-macs

no allow non-profiled-macs

Command Default

Non-profiled MAC addresses are not dropped.

Modes

Port-profile mode

Usage Guidelines

This configuration is allowed on the default profile only.

Enter **no allow non-profiled-macs** to return to the default setting.

Examples

```
switch(config)# port-profile default

switch(config-port-profile-default)# allow non-profiled-macs
```

always-compare-med

Configures the device always to compare the Multi-Exit Discriminators (MEDs), regardless of the autonomous system (AS) information in the paths.

Syntax

always-compare-med

no always-compare-med

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To configure the device always to compare the MEDs:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# always-compare-med
```

always-propagate (BGP)

Enables the device to reflect routes even though they are not installed in the Routing Table Manager (RTM).

Syntax

always-propagate

no always-propagate

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To configure the device to reflect routes that are not installed in the RTM:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# always-propagate
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

area authentication (OSPFv3)

Enables authentication for an Open Shortest Path First (OSPF) area.

Syntax

area { *A.B.C.D* | *decimal* } **authentication spi** *spi* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** [**no-encrypt**] *key*

no area { *A.B.C.D* | *decimal* } **authentication spi** *spi*

Command Default

Authentication is not enabled on an area.

If the **no-encrypt** keyword is not used, the key is stored in encrypted format by default.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

spi
Specifies the Security Policy Index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah
Specifies authentication header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key
Number used in the calculation of the message digest. The 40 hexadecimal character key is stored in encrypted format by default.

no-encrypt
The 40-character key is not encrypted upon either its entry or its display.

key
The 40 hexadecimal character key.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no area authentication spi** to remove an authentication specification for an area from the configuration.

The 40 hexadecimal character key is encrypted by default. Use the **no-encrypt** parameter to disable encryption.

Examples

To enable ah and MD5 authentication for an OSPF area, setting a SPI value of 750:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip router-id 10.1.2.3
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 750 ah hmac-md5 key
abcef12345678901234fedcba098765432109876
```

To enable esp and SHA-1 authentication for an OSPF area, setting a SPI value of 900:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip router-id 10.1.2.3
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 750 esp null hmac-md5 sha1
abcef12345678901234fedcba098765432109876
```

History

Release version	Command history
5.0.1a	This command was introduced.

area nssa (OSPF)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *A.B.C.D* | *decimal* } **nssa** { *metric* [**no-summary**] | **default-information-originate** }

no area nssa

Command Default

No areas are created.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address In decimal format.

metric
Additional cost for using a route to or from this area.

no-summary
When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA an NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs.
Note: This parameter is disabled by default, which means the default route must use a Type 7 LSA.

default-information-originate
When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

Modes

OSPF VRF router configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

Enter **no area nssa** to delete an NSSA.

Examples

To set an additional cost of 5 on an NSAA identified as 2 (in decimal format), and include the no-summary parameter:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)#router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 nssa 5 no-summary
```

area nssa (OSPFv3)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *A.B.C.D* | *decimal* } **nssa** [*metric*] [**default-information-originate** [**metric** *num* | **metric-type** { **type-1** | **type-2** }]] [**no-redsitribution**] [**no-summary**] [**translator-always**] [**translator-interval** *interval*]

no area nssa

Command Default

No areas are created.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

metric
Additional cost for using a route to or from this area. Valid values range from 1 through 1048575.

default-information-originate
When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

metric-type
Specifies how the cost of a neighbor metric is determined. The default is type-1.

type-1
The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

type-2
The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

no-redistribution
The no-redistribution parameter prevents an NSSA ABR from generating external (type-7) LSA into an NSSA area. This is used in the case where an ASBR should generate type-5 LSA into normal areas and should not generate type-7 LSA into NSSA area. By default, redistribution is enabled in a NSSA.

no-summary
When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA an NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs.
Note: This parameter is disabled by default, which means the default route must use a Type 7 LSA.

translator-always

Configures the translator-role. When configured on an ABR, this causes the router to unconditionally assume the role of an NSSA translator. By default, translator-always is not set, the translator role by default is candidate.

translator-interval *interval*

Configures the time interval for which an elected NSSA translator continues to perform its duties even after its NSSA translator role has been disposed by another router. By default the stability-interval is 40 seconds and its range is 10 to 60 seconds.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

Enter **no area nssa** to delete an NSSA.

Examples

To set an additional cost of 4 on an NSAA identified as 8 (in decimal format), and prevent any Type 3 or Type 4 summary LSAs from being injected into the area:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)#ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 8 nssa 4 no-summary
```

History

Release version	Command history
5.0.0	This command was introduced.

area range (OSPF)

Specifies area range parameters on an Area Border Router (ABR).

Syntax

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* { **advertise** | **not-advertise** } [**cost** *cost_value*]

no area range

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

E.F.G.H I.J.K.L
Specifies the IPv6 address and mask portion of the range. All network addresses that match this network are summarized in a single route and advertised by the ABR.

advertise
Sets the address range status to *advertise* and generates a Type 3 summary LSA.

cost *cost_value*
Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for *cost_value* is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.

not-advertise
Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command only on ABRs to specify route summarization for an existing area. The result is that a single summary route is advertised to other areas by the ABR, in the form of a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only a single route is advertised for each address range.

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

Enter **no area range** to disable the specification of range parameters on an ABR

Examples

To advertise to Area 3 all the addresses on the network 1.1.1.0 255.255.255.0 in the ABR you are signed into:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 3 range 1.1.1.0 255.255.255.0 advertise
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

area stub (OSPF)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *A.B.C.D* | *decimal* } **stub** *metric* [**no-summary**]

no area stub

Command Default

No areas are created.

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address In decimal format.

metric

Additional cost for using a route to or from this area. Valid values range from 3 through 1048575.

no-summary

When configured on the ABR, prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

Enter **no area stub** to delete a stub area.

Examples

To set an additional cost of 5 on a stub area called 2 (in decimal format):

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 stub 5
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

area virtual-link (OSPF)

Creates or modifies virtual links for an area.

Syntax

area { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* [**authentication-key** { 0 | 2 | 255 } *password*] [**dead-interval** *time*] [**hello-interval** *time*] [**md5-authentication** { **key-activation-wait-time** *time* | **key-id** *num key* }] [**retransmit-interval** *time*] [**transmit-delay** *time*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

E.F.G.H
ID of the OSPF router at the remote end of the virtual link.

authentication-key
Sets the password and encryption method. Only one encryption method can be active on an interface at a time. All OSPF packets transmitted on the interface contain this password. All OSPF packets received on the interface are checked for this password. If the password is not present, then the packet is dropped.

0
Does not encrypt the password you enter.

2
Encrypts the password you enter.

255
Encrypts a plain-text password that you enter.

password
OSPF password. The password can be up to eight alphanumeric characters.

dead-interval *time*
How long a neighbor router waits for a hello packet from the current router before declaring the router down. This value must be the same for all routers and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval
Time between hello packets that the router sends on an interface. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

md5-authentication

Sets either MD5 key-activation wait time or key identifier.

key-activation-wait-time *time*

Time before a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes (300 seconds) after the new MD5 key is in operation. Valid values range from 0 through 14400 seconds. The default is 300 seconds.

key-id *num key*

The *num* is a number between 1 and 255 which identifies the MD5 key being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the key is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

retransmit-interval *time*

Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two routers on the attached network. Valid values range from 0 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

Modes

OSPF VRF router configuration mode

Usage Guidelines

Enter **no area virtual-link** to remove a virtual link.

Examples

To create a virtual link for an area whose decimal address is 1, and where the ID of the OSPF router at the remote end of the virtual link is 10.1.2.3:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.1.2.3
```

area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

Syntax

area { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* [**dead-interval** *time*] [**hello-interval** *time*] [**hello-jitter** *interval*] [**retransmit-interval** *time*] [**transmit-delay** *time*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format.

E.F.G.H

ID of the OSPFv3 router at the remote end of the virtual link.

dead-interval *time*

How long a neighbor router waits for a hello packet from the current router before declaring the router down. This value must be the same for all routers and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval

Time between hello packets that the router sends on an interface. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

hello-jitter

Sets the allowed jitter between hello packets. Valid values range from 1 through 50 percent (%). The default value is 10%.

retransmit-interval *time*

Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two routers on the attached network. Valid values range from 0 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second..

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no area virtual-link** to remove a virtual link.

Examples

To create a virtual link for an area whose decimal address is 1, and where the ID of the OSPFv3 router at the remote end of the virtual link is 209.157.22.1:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 209.157.22.1
```

History

Release version	Command history
5.0.0	This command was introduced.

area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPF area.

Syntax

area { *A.B.C.D* | *decimal* } **virtual-link authentication spi** *spi* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** [**no-encrypt**] *key*

no area { *A.B.C.D* | *decimal* } **virtual-link authentication spi** *spi*

Command Default

Authentication is not enabled on a virtual-link.

The 40 hexadecimal character key is encrypted by default. Use the **no-encrypt** parameter to disable encryption.

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

spi
Specifies the security policy index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah
Specifies authentication header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key
Number used in the calculation of the message digest. The 40 hexadecimal character key is stored in encrypted format by default.

no-encrypt
The 40-character key is not encrypted upon either its entry or its display.

key
The 40 hexadecimal character key.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no area** { *A.B.C.D* | *decimal* } **virtual-link authentication spi** *spi* to remove authentication from the virtual-links in the area.

Examples

To configure IPsec on a virtual link in an OSPF area:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip router-id 10.1.2.2
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2 virtual-link 10.1.2.2 authentication spi 600 ah
hmac-sha1 no-encrypt key 113456789022345678901234567890123456789O
```

History

Release version	Command history
5.0.1a	This command was introduced.

arp

Enables specification of an IPv4 address for an Address Resolution Protocol (ARP) entry.

Syntax

arp *A.B.C.D mac_address* [**ve** *vlan_id* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

A.B.C.D
A valid IP address.

mac_address
A valid MAC address.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve *vlan_id*
Specifies the corresponding VLAN interface that must already be configured before the VE interface can be created. Refer to the Usage Guidelines.

Modes

RBridge ID configuration mode

Usage Guidelines

Before you can configure a VE interface, you must configure a VLAN interface. The corresponding VE interface must use the same VLAN ID you used to configure the VLAN.

Enter **no interface ve** *vlan_id* to remove the VE interface. This will not remove the corresponding VLAN interface.

CAUTION
If no RBridge ID is configured on the switch, deleting the VE interface will cause a spike in CPU usage. To prevent this, configure an RBridge ID before deleting the VE interface.

as-path-ignore

Disables the comparison of the autonomous system (AS) path lengths of otherwise equal paths.

Syntax

as-path-ignore

no as-path-ignore

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To configure the device always to disable the comparison of AS path lengths:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# as-path-ignore
```

attach rbridge-id

Assigns a range of RBridge IDs to a VXLAN gateway instance.

Syntax

attach rbridge-id { **add** | **remove** } *rb-range*

Parameters

add

Attaches a specified range of RBridge IDs to a VXLAN gateway.

remove

Un-attaches a specified range of RBridge IDs from a VXLAN gateway.

rb-range

Specifies a range of RBridge IDs to attach to the VXLAN gateway, up to a maximum of four RBridge IDs. (You can also specify just one RBridge ID.) Ranges can be specified by hyphens, separated by commas, or contain a mixture of both.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

This command is allowed for a switch that is in logical chassis cluster mode only.

Use the **add** form of the command to attach RBridge IDs to the VXLAN gateway, and use the **remove** form of the command to unattach RBridge IDs from the VXLAN gateway. The maximum number of RBridge IDs that can be attached is four.

When unattaching RBridge IDs, gateway and tunnel configurations on the specified RBridge IDs are deleted.

You can configure other properties for the gateway instance while in VXLAN overlay gateway configuration mode, but the gateway instance is not created until you enter the **attach rbridge-id** command. Do not use a space after a comma when specifying a range of RBridge IDs. For example, to specify RBridges 5 through 7 and RBridge 9, enter the following: 5-7,9.

The RBridge IDs that you specify must already be known to the cluster. (RBridge IDs that have been removed from the cluster by means of the **no vcs enable rbridge-id** command cannot be used to attach to the VXLAN gateway.)

The RBridge IDs that you specify must be on a VXLAN-capable gateway (either the Brocade VDX 6740 or VDX 6740-T).

Examples

To add an RBridge ID range of 10 through 12 on a VXLAN overlay gateway instance named "gateway1":

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# attach rbridge-id add 10-12
```

Related Commands

overlay-gateway, rbridge-id

attach rbridge-id (Fabric-Virtual-Gateway)

Assigns a range of RBridge IDs to the global VE interface.

Syntax

attach rbridge-id { **add** | **remove** } *rb-range*

Command Default

None

Parameters

add

Attaches a specified range of RBridge IDs to the VE interface.

remove

Removes a specified range of RBridge IDs from the VE interface.

rb-range

Specifies a range of RBridge IDs to attach to the VE interface, up to a maximum of four RBridge IDs. (You can also specify a single RBridge ID.) Ranges can be specified by hyphens, separated by commas, or contain a mixture of both.

Modes

Fabric-Virtual-Gateway global VE interface configuration mode

Usage Guidelines

Use the **add** form of the command to attach RBridge IDs to the VE interface, and use the **remove** form of the command to unattach RBridge IDs from the VE interface. The maximum number of RBridge IDs that can be attached is four.

Examples

The following example shows how to attach an RBridge-ID to the VE interface.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# attach rbridge-id add 54,55
```

History

Release version	Command history
5.0.1	This command was introduced.

attach vlan

Identifies exported VLANs in VXLAN gateway configurations.

Syntax

attach vlan *vlan_ID* [**mac** *mac_address*]

no attach vlan *vlan_ID*

Parameters

vlan *vlan_ID*
Specifies the VLAN ID of the VXLAN gateway. This can be a range, such as 5, 10, 20-25.

mac *mac_address*
Specifies the MAC address of a VXLAN gateway, in *HHHH.HHHH.HHHH* format.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Exported VLANs are VLANs than can be mapped to VXLAN domains. All the MAC addresses that the VXLAN gateway learns on these VLANs are shared with the NSX controller.

This command is applicable only when the gateway type is **nsx**, as configured by means of the **overlay-gateway** command.

This command can optionally accept specific MAC addresses, which can be shared with the NSX Controller. If the user specifies MAC addresses, only the specified MAC addresses are shared with the NSX Controller for the specified VLAN. The specified VLAN must already be configured.

You cannot run two forms of this command that use the same VLAN IDs. For example, the commands **attach vlan** *x* and **attach vlan** *x***mac** *y* cannot coexist. If one form of the configuration exists, the other form of the configuration that uses the same VLAN ID is rejected.

Also, you cannot specify a VLAN range and a MAC address on the same command line. You can, however, specify a single VLAN ID and a MAC address on the same command line.

The **no** form of this command stops the MAC addresses behind the specified VLANs from being shared with the NSX Controller.

The deletion of a VLAN specified by this command is not allowed. For example, if you enter the **attach vlan** *x* command, you cannot delete the exported VLAN called x by running the **no interface vlan** *x* command.

Examples

To specify an exported VLAN ID and a MAC address for a VXLAN gateway named "gateway1" that is already configured:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# attach vlan 5 mac 00:05:1e:c5:96:a4
```

Related Commands

overlay-gateway

auto-cost reference-bandwidth (OSPF)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth { *ref-bw* | **use-active-ports** }

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

ref-bw

Reference bandwidth in Mbps. Valid values range from 1 through 4294967.

use-active-ports

When set, any dynamic change in bandwidth immediately affects the cost of OSPF routes. This parameter enables cost calculation for currently active ports only.

Modes

OSPF VRF router configuration mode

Usage Guidelines

OSPF calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

NOTE

If you specify the cost for an individual interface (by using the **ip ospf cost** command), the cost you specify overrides the cost calculated by the software.

Enter **no auto-cost reference-bandwidth** to disable bandwidth configuration.

Examples

To change a reference bandwidth of 500:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

Related Commands

ip ospf cost

auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth { *ref-bw* }

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

ref-bw

Reference bandwidth in Mbps. Valid values range from 1 through 4294967.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

OSPFv3 calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

NOTE

If you specify the cost for an individual interface (by using the **ipv6 ospf cost** command), the cost you specify overrides the cost calculated by the software.

Enter **no auto-cost reference-bandwidth** to disable bandwidth configuration.

Examples

To change a reference bandwidth to 500:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-5)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

- The reference bandwidth specified in this example results in the following costs:10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.
- 155 Mbps port cost = 500/155 = 3.23, which is rounded up to 4
- 622 Mbps port cost = 500/622 = 0.80, which is rounded up to 1
- 2488 Mbps port cost = 500/2488 = 0.20, which is rounded up to 1

The costs for 10 Mbps, 100 Mbps, and 155 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

ipv6 ospf cost

backup-advertisement-interval

Configures the interval at which backup VRRP routers advertise their existence to the master router.

Syntax

backup-advertisement-interval *interval*

Command Default

60 seconds

Parameters

interval

Interval at which a backup VRRP router advertises its existence to the master router. Valid values range from 60 through 3600 seconds.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The interval is the length of time, in seconds, between each advertisement sent from the backup routers to the master router. The advertisement notifies the master router that the backup is still active. If the master router does not receive an advertisement from the backup in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E.

Examples

To set the backup advertisement interval to 120 seconds for VRRP-E group 10:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-extended-group 10
switch(config-vrrp-extended-group-10)# backup-advertisement-interval 120
```

Related Commands

vrrp-extended-group, vrrp-group

banner incoming

Sets the incoming banner message.

Syntax

banner incoming *message*

no banner incoming

Parameters

message

The message string to be displayed on the switch console.

Modes

Global configuration mode

Usage Guidelines

A banner is a text message that displays on the console. The banner can include information about the switch for a user to know when accessing the switch.

The banner must be from 1 through 2048 characters in length. The banner can appear on multiple lines if you enter multiline mode using **ESC+M** and using **CTRL+D** to exit.

banner login

Sets the switch banner.

Syntax

banner login *message*

no banner login

Parameters

message

The message string to be displayed on the switch console.

Modes

Global configuration mode

Usage Guidelines

A banner is a text message that displays on the console. The banner can include information about the switch that a user wants another user to know when accessing the switch.

The banner must be from 1 through 2048 characters in length.

The banner can appear on multiple lines if you enter multiline mode using **ESC-M** and using **CTRL-D** to exit.

Examples

To create a banner with multiple lines:

```
switch(config)# banner login [Esc-m]

[Entering multiline mode, exit with ctrl-D.]
> banner login Hello
> and
> welcome
> to
> the
> switch
[Ctrl-D]
switch(config)# do show running-config banner

banner login "Hello\and\welcome\to\the\switch"

switch(config)# exit

Network OS (switch)
NOS Version 3.0.0
switch login: admin

Password: ******

Hello and welcome to the switch
```

To create a banner with a single line:

```
switch(config)# banner login "Please do not disturb the setup on this switch"

switch(config)# exit

Login: user

Password: *****

The cluster contains 5 switches
---------------
Welcome to NOS CLI
user connected from ::FFFF:10.103.8.61 using ssh on abc.com
switch#
```

Related Commands

show running-config banner

banner motd

Sets the message of the day (MOTD) banner.

Syntax

banner motd *message*

no banner motd

Parameters

message

The message string to be displayed on the switch console.

Modes

Global configuration mode

Usage Guidelines

A banner is a text message that displays on the console. The banner can include information about the switch for a user to know when accessing the switch.

The banner must be from 1 through 2048 characters in length. The banner can appear on multiple lines if you enter multiline mode by using **ESC+M** and exit by using **CTRL+D** .

bgp-redistribute-internal

Causes the device to allow the redistribution of IBGP routes from BGP4 and BGP4+ into RIP, OSPF, or IS-IS.

Syntax

bgp-redistribute-internal

no bgp-redistribute-internal

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

By default, with default VRF instances, the device does not allow the redistribution of IBGP routes from BGP4 and BGP4+ into RIP, OSPF, or IS-IS. This helps to eliminate routing loops. In non-default VRF instances, the device does allow the redistribution of IBGP routes from BGP4 and BGP4+ into RIP and OSPF.

Use the **no** form of the command to restore the defaults.

Examples

To configure a static network and change the administrative distance:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# bgp-redistribute-internal
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

bind

Creates a persistent binding between the logical FCoE port and the ten/forty gigabit or LAG port.

Syntax

bind { <*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **mac-address** *address* }

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel interface.

mac-address *address*

Specifies a MAC address. The valid format is HH:HH:HH:HH:HH:HH.

Modes

Interface subtype configuration mode

Usage Guidelines

The configuration will be stored in the configuration and retained across reboots.

When the FCoE logical port is automatically bound to a TE/FO LAG port, it is referred as dynamic binding. This binding is valid only till the FLOGI session is valid. The binding is automatically removed when CNA logs out.

ATTENTION

Only one type of binding can be used for each physical port, so the ten/forty gigabit Ethernet or LAG (MAC) binding configurations overwrite each other.

Examples

```
switch(config)# interface fcoe 1/1/55
switch(config-Fcoe-1/1/55)# bind tengigabitethernet 1/0/1
switch(config)# interface fcoe 1/1/56
switch(config-Fcoe-1/1/56)# bind mac-address 00:05:1e:c5:96:a4
```

bpdu-drop enable

Drops STP, RSTP, MSTP, and PVST and RPVST bridge protocol data units (BPDUs), disabling the tunneling of those protocols on an interface.

Syntax

bpdu-drop enable [**rx** | **tx** | **all**]

no bpdu-drop enable [**rx** | **tx** | **all**]

Command Default

BPDU-drop is disabled.

Parameters

t x
: Disables tunneling in the transmit direction.

rx
: Disables tunneling in the receive direction.

all
: Disables tunneling in both the transmit and receive directions.

Modes

Interface subtype configuration mode

Usage Guidelines

This command prevent reception of any STP or PVST BPDUs on a interface. If such a BPDU is received on a interface that is BPDU-drop enabled, the interface drops the BPDU frames, but does not shut down.

Enter **bpdu-drop enable** with the **tx**, **rx**, or **all** options. Without an optional keyword, the action applies to the ingress direction only.

Enter **no bpdu-drop enable** with the **tx**, **rx**, or **all** options to disable BPDU drop in one or more directions.

Enter **no bpdu-drop enable** to disable BPDU-drop completely.

Examples

To enable BPDU-drop on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet178/0/9
switch(conf-if-te-178/0/9)# bpdu-drop enable
```

To disable BPDU-drop on a specific port-channel interface:

```
switch(config)# interface port-channel 62
switch(conf-port-channel-62)# no bpdu-drop enable
```

To disable BPDU-drop on a specific port-channel interface in the transmit direction:

```
switch(config)# interface port-channel 62
switch(conf-port-channel-62)# no bpdu-drop enable tx
```

Related Commands

interface

bridge-priority

Specifies the bridge priority for the common instance.

Syntax

bridge-priority *priority*

no bridge-priority

Command Default

Priority is 32768.

Parameters

priority

Specifies the bridge priority. Valid values range from 0 through 61440 in increments of 4096.

Modes

Protocol Spanning Tree mode

Usage Guidelines

The priority values can be set only in increments of 4096.

Using a lower priority value indicates that the bridge might become root.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Enter **no bridge-priority** to return to the default priority.

Examples

To specify the bridge priority:

```
switch# configure terminal
switch(config)# protocol spanning-tree stp
switch(conf-stp)# bridge-priority 8192
switch# configure terminal
switch(config)# protocol spanning-tree rstp
switch(conf-rstp)# bridge-priority 8192
switch# configure terminal
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# bridge-priority 8192
```

Related Commands

protocol spanning-tree

capability as4

Enables 4-byte autonomous system number (ASN) capability at the BGP global level.

Syntax

capability as4 enable

no capability as4

Command Default

This feature is disabled.

Parameters

enable

Enables 4-byte ASN capability at the BGP global level.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

To enable 4-byte ASN capability:

```
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# capability as4 enable
```

capture packet interface

Enables the capture of packet information on an interface, for display on the switch itself or for storage in an automatically generated file.

Syntax

capture packet { **interface** } { **all** | *<N>***gigabitethernet** *rbridge-id/slot/port* } { **direction** { **both** | **rx** | **tx** }} { **filter** { **l2** | **l3** | **all** }

Parameters

interface

Selects an interface (required).

all

Selects all interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

direction

Selects a direction (required).

both

Selects traffic in both transmit and receive directions.

rx

Selects received traffic.

tx

Selects transmitted traffic.

filter

Selects the packet types to be filtered (required).

l2

Filters only Layer 2 packets to the CPU.

l3

Filters only Layer 3 packets to the CPU.

all

Filters all packets to the CPU, including transit packets if an access control list (ACL) is enabled (Refer to the Usage Guidelines.)

Modes

Privileged EXEC mode

Usage Guidelines

Capturing packet information on an interface can provide significant help in debugging, especially for Layer 2 TRILL and Layer 3 packets. Captured packets are stored in a circular buffer, and they are also written to an automatically generated "pktcapture.pcap" file, which can store up to 1500 K of data in flash memory (the equivalent of approximately 10k packets, each having an average size of 100 bytes). Once this file is full, it is saved at *_old.pcap and data are written to a new pktcapture.pcap file. These files can be exported and viewed through a packet analyzer such as Wireshark.

NOTE
Up to 100 packets per interface can be captured. Once the buffer is filled, the oldest packets are replaced with the most recent.

This command can be entered on any RBridge in a Brocade VCS Fabric.

To disable packet capture globally, use the **no capture packet all** command.

NOTE
The **all** option is not supported for enabling packet capture.

To view the captured information on the switch, use the **show capture packet interface** command.

Note the following limitations:

- Support is provided only on physical (Ethernet) interfaces, not on logical interfaces. To see packets on logical interfaces, first enable the capture on the corresponding physical interfaces.
- In the initial release, support for capturing transit traffic requires ACL logging.
- Packets that are dropped in the ASIC cannot be captured.

CAUTION
Capturing packets over multiple sessions and over long durations can affect system performance.

Examples

```
switch# capture packet interface tengigabitethernet 166/0/1 direction both filter all
```

Related Commands

show capture packet interface

cbs

Mandatory command for configuring the controlled burst size for a class-map.

Syntax

cbs *cbs-size*

no cbs *cbs-size*

Parameters

cbs-size

Controlled burst size. Valid values range from 1250 through 5000000000 bytes in increments of 1 byte. This is a mandatory parameter for configuring a class-map.

Modes

Policymap class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal

switch(config)# policy-map policymap1

switch(config-policymap)# class default

switch (config-policymap-class)# police cir 40000

switch(config-policymap-class-police)# cbs 50000
```

cee

Applies a Converged Enhanced Ethernet (CEE) provisioning map on an interface.

Syntax

cee *default*

no cee

Command Default

There is no CEE provisioning applied on an interface. The only map name allowed is "default."

Modes

Interface subtype configuration mode

Usage Guidelines

The CEE map applied on an interface should already exist on the switch.

Enter **no cee** to remove the CEE provisioning map.

Examples

To apply a CEE map to a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# cee default
```

cee-map (configuration)

Enters the CEE map configuration mode.

Syntax

cee-map default

Command Default

The only map name allowed is "default."

Modes

Global configuration mode

Usage Guidelines

Only a single CEE map is allowed, named "default." It is created when system starts up. The initial configuration of the default CEE map is:

```
Precedence 1
  Priority Group Table
     1:  Weight 40, PFC Enabled, BW% 40
     2:  Weight 60, PFC Disabled, BW% 60
     15.0: PFC Disabled
     15.1: PFC Disabled
     15.2: PFC Disabled
     15.3: PFC Disabled
     15.4: PFC Disabled
     15.5: PFC Disabled
     15.6: PFC Disabled
     15.7: PFC Disabled
   Priority Table
      CoS:    0    1    2    3    4    5    6    7
     ---------------------------------------------
     PGID:    2    2    2    1    2    2    2    2
   Enabled on the following interfaces
```

Related Commands

cee, fcoeport, priority-group-table

cee-map (FCoE)

Assigns a CEE map to the FCoE Fabric-Map.

Syntax

cee-map default

no cee-map default

Command Default

The only map name allowed is "default."

Modes

FCoE map configuration mode

Usage Guidelines

You must be in the feature configuration mode for FCoE map for this command to function.

Enter **no cee-map** to revert to the default values for the map.

Examples

```
switch(config)# fcoe
switch(config-fcoe)# map default
switch(config-fcoe-map)# cee-map default
```

Related Commands

fabric-map, fcoe

certutil import ldapca

Imports a Lightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate from a remote server

Syntax

certutil import ldapca directory *path* **file** *filename* **protocol** { *FTP* | *SCP* } **host** *remote_ip* **user** *user_acct* **password** *password* **ssh**

certutil import ldapca | **syslogca directory** *ca certificatepath* **protocol** { *FTP* | *SCP* } **host** *remote_ip* **user** *user_acct* **password** *password* [**rbridge-id** { *rbridge_id* | **all** }]

no certutil ldapca [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

directory *path*
Specifies the path to the certificate.

file *filename*
Specifies the filename for the certificate.

host *remote_ip*
Specifies the IP address of the remote host.

password *password*
Specifies the password to access the remote host.

protocol *FTP* | *SCP*
Specifies the protocol used to access the remote server.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

all
Specifies all RBridges.

user *user_acct*
Specifies the user name to access the remote host.

Modes

Privileged EXEC mode

Usage Guidelines

This command supports FTP and SCP.

Enter **no certutil ldapca** to delete the LDAP CA certificates of all Active Directory (AD) servers.

Examples

To import the SSH public key for user "admin" from the remote host:

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh file
id_rsa.pub login fvt
Password: ***********
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil, Status: success, Info:
Imported SSH public key from 10.70.4.106 for user 'admin'.
switch#
```

To delete all LDAP CA certificates:

```
switch# no certutil ldapca
```

In VCS mode

To import a certificate for LDAP:

```
switch# certutil import ldapca directory /usr/ldapcacert/ file cacert.pem protocol SCP host 10.23.24.56
user admin password rbridge-id 3
password:
switch#
```

To delete LDAP certificates on rbridge-id 3:

```
switch# no certutil syslogca rbridge-id 3
Do you want to delete syslogca certificate? [y/n]:y
Warning: All the syslog CA certificates are deleted.
switch
```

certutil import sshkey

Imports the SSH public key for an SSH user from the remote host using the mentioned login credentials and path name.

Syntax

certutil import sshkey host *remote_ip_address* **directory** *ssh_public_key_path* **user** *user_acct* **password** *password* **login** *login_id* [**rbridge-id** { *rbridge-id* | **all** }]

no certutil sshkey [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

directory *path*
Specifies the path to the certificate.

file *filename*
Specifies the SSH public key with a .pub extension.

host *remote_ip*
Specifies the IP address of the remote host.

login *login_id*
Specifies the login name in the remote host.

password *password*
Specifies the password to access the remote host.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

user *user_acct*
Specifies the user name to access the remote host.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no certutil sshkey user** to delete the SSH public key a specified user.

Examples

The following command deletes the SSH public key for "testuser."

```
switch# no certutil sshkey user testuser
 Do you want to delete the SSH public key file? [y/n]:y
switch# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, VDX6720-24, Event: sshutil, Status: success,
Info: Deleted SSH public keys associated to user 'testuser'.
```

In VCS mode

The following command imports a public CA certificate:

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh file
id_rsa.pub login fvt rbridge-id 3
Password: ***********
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil, Status: success, Info:
Imported SSH public key from 10.70.4.106 for user 'admin'.
```

The following command deletes the SSH public key for "testuser."

```
switch# no certutil sshkey user testuser rbridge-id 3
 Do you want to delete the SSH public key file? [y/n]:y
switch# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, VDX6720-24, Event: sshutil, Status: success,
Info: Deleted SSH public keys associated to user 'testuser'.
```

Related Commands

show cert-util sshkey

certutil import syslogca

Imports a syslog CA certificate.

Syntax

certutil import syslogca directory *path* **file** *filename* **protocol** { *FTP* | *SCP* } **host** *remote_ip* **user** *user_acct* **password** *password* [**rbridge-id** { *rbridge-id* | **all** }]

no certutil syslogca

Parameters

directory *path*
Specifies the path to the certificate.

file *filename*
Specifies the filename for the certificate.

host *remote_ip*
Specifies the IP address of the remote host.c

password *password*
Specifies the password to access the remote host.

protocol *FTP* | *SCP*
Specifies the protocol used to access the remote server.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

user *user_acct*
Specifies the user name to access the remote host.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no certutil syslogca** to delete the syslog CA certificates of all Active Directory servers.

Examples

The following command deletes a syslog CA certificate:

```
switch# no certutil syslogca
 Do you want to delete syslog CA certificate? [y/n]:

In VCS mode
```

The following command imports a syslog CA certificate:

```
switch# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem protocol SCP host
10.23.24.56 user admin password rbridge-id 3
password:
switch#
```

The following command deletes a syslog CA certificate:

```
switch# no certutil syslogca rbridge-id 5
 Do you want to delete syslog CA certificate? [y/n]:
```

channel-group

Enables Link Aggregation on an interface.

Syntax

channel-group *number* **mode** { **active** | **passive** | **on** } [**type** { **standard** | **brocade** }]

no channel-group

Command Default

The value for **type** is set to **standard**.

Parameters

number

Specifies a Link Aggregation Group (LAG) port channel-group number to which this link should administratively belong to. Valid values range from 1 through 6144.

mode

Specifies the mode of Link Aggregation.

active

Enables the initiation of LACP negotiation on an interface.

passive

Disables LACP on an interface.

on

Enables static link aggregation on an interface.

type

Specifies the type of LAG.

standard

Specifies the 802.3ad standard-based LAG.

brocade

Specifies the Brocade proprietary hardware-based trunking.

Modes

Interface subtype configuration mode

Usage Guidelines

This command adds an interface to a port-channel specified by the channel-group number. This command enables link aggregation on an interface, so that it may be selected for aggregation by the local system.

Only a maximum of 24 LAGs can be created. Be aware of the following:

- A maximum of four link aggregation groups can be created per switch when the **type** is set to **brocade**.

- A maximum of four links can become part of a single aggregation group when the **type** is set to **brocade** and they must be on the same port-channel.
- Links 0 through 7 belong to port-channel 1; links 8 through 15 belong to port-channel 2, and links 16 through 23 belong to port-channel 3.
- For the **standard** type, a maximum of 16 links can be aggregated per aggregation group and they can be members of any port-channel.
- Enter **no channel-group** to remove the port-channel members.

NOTE
For additional discussion of using the **channel-group** command,

Network OS Layer 2 Switching Configuration Guide

Examples

To set the channel-group number to 4 and the mode to *active* on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# channel-group 4 mode active
```

To set the channel-group number to 10, the mode to *passive* , and the type to brocade on a specific 1-gigabit Ethernet interface:

```
switch(config)# interface gigabitethernet 170/0/1
switch(conf-if-gi-170/0/1)# channel-group 10 mode passive brocade
```

History

Release version	Command history
5.0.1	This command was updated with a reference to the *Network OS Layer 2 Switching Configuration Guide*.

Related Commands

interface

chassis

Sets the IPv4 or IPv6 address of a switch chassis.

Syntax

chassis { **virtual-ip** | **virtual-ipv6** }

no chassis { **virtual-ip** | **virtual-ipv6** }

Parameters

virtual-ip
Sets an IPv4 address in dotted-decimal notation with a CIDR prefix (mask).

virtual-ipv6
Sets an IPv6 address in colon-separated hexadecimal notation with a CIDR prefix.

Modes

RBridge ID configuration mode

Usage Guidelines

This command changes the default chassis IPv4 or IPv6 address. The default is the initial address of the switch chassis.

This is the address that is used to access devices through their RBridge ID. Use this command to change the IP address to facilitate management, for example, if a switch is moved to a different subnet. The IP address of the management platform should be in the same subnet as the devices it manages.

This command applies only to chassis switches, for example, the Brocade VDX 8770.

Use the **no** form of this command to revert to the default address.

Examples

IPv4:

```
switch(config)# rbridge-id 4
switch(config-rbridge-id-4)# chassis virtual-ip 10.11.12.13/20
```

IPv6:

```
switch(config)# rbridge-id 4
switch(config-rbridge-id-4)# chassis virtual-ipv6 2001:db8:8086:6502/64
```

Related Commands

show rbridge-id, show running-config

chassis beacon

Controls the flashing LED beacon on the switch which makes finding the desired switch easier in large data centers.

Syntax

chassis beacon { **enable** | **disable** }

Parameters

enable

Enables the chassis beacon LED.

disable

Disables the chassis beacon LED.

Modes

Privileged EXEC mode

Examples

To enable the chassis beacon:

```
switch# chassis beacon enable
Chassis Beacon has been enabled
```

To disable the chassis beacon:

```
switch# chassis beacon disable
Chassis Beacon has been disabled
```

chassis disable

Disables all interfaces in the chassis.

Syntax

chassis disable

Modes

Privileged EXEC mode

Usage Guidelines

All interfaces will be taken offline

This command is supported only on the local switch.

Enter **chassis disable** before making configuration changes or running offline diagnostics.

You must execute the **chassis enable** command after running offline diagnostics, or the switch will not boot correctly.

Examples

To disable all interfaces on the local switch:

```
switch# chassis disable
```

Related Commands

chassis enable

chassis enable

Enables all interfaces in the chassis.

Syntax

chassis enable

Modes

Privileged EXEC mode

Usage Guidelines

All interfaces that passed the power-on self-test (POST) are enabled. They may come online if connected to a device, or remain offline if disconnected. Enter **chassis enable** to re-enable the chassis after making configuration changes or running offline diagnostics.

This command is supported only on the local switch.

You must execute the **chassis enable** command after running offline diagnostics, or the switch will not boot correctly.

Examples

To enable all interfaces on the local switch:

```
switch# chassis enable
```

Related Commands

chassis disable

chassis fan airflow-direction

Specifies the direction of airflow through the chassis based on physical PSU and fans.

Syntax

chassis fan airflow-direction [**port-side-intake** | **port-side-exhaust**]

Parameters

port-side-intake
Specifies the airflow to enter the switch.

port-side-exhaust
Specifies the airflow to exit the switch.

Modes

Global configuration mode

Usage Guidelines

This command must only be used after you purchase and install the appropriate fan/power supply that provides the desired airflow direction in the switch. Please contact your Brocade Sales Representative to obtain the correct part numbers and pricing.

When the **chassis fan airflow-direction** command is issued, the switch will not recognize the configuration change until the switch is rebooted.

Only one (1) configuration change is accepted per reboot. This means that even if this command is entered multiple times, only the first configuration change entered will be effective after rebooting.

The switch serial number is registered with Brocade and the information recorded in the Brocade database about that switch includes the airflow orientation at the time of shipment. Any subsequent change in airflow direction is not recorded in the Brocade database. This means that if you request a Return Merchandise Authentication (RMA) for the switch, the replacement switch will be sent with the original orientation.

Examples

To specify the fan airflow-direction:

```
switch# chassis fan airflow-direction port-side-exhaust

Previous configuration : port-side-intake
Current configuration  : port-side-exhaust
System fan airflow-direction changes will be effective after reboot!!
```

cidrecov

Recovers data from Chassis ID cards if possible.

Syntax

cidrecov

Modes

Privileged EXEC mode

Usage Guidelines

Use this command if you receive an error or warning RASLog message that instructs you to run this command.

Two chassis ID (CID) cards contain data necessary for system operation. Each CID contains two Serial Electronically Erasable Programmable Read Only Memory (SEEPROM) devices. If data on either card becomes corrupt or mismatched, a regularly run CID audit writes messages to the RASLog. Follow the instructions in the messages. Mismatched data can be reset, and corrupt data can sometimes be recovered if the corrupt data is on the non-critical SEEPROM.

This command is supported only on Brocade VDX 8770-4 and Brocade VDX 8770-8 switches.

Examples

Example 1: Noncritical SEEPROM is inaccessible or corrupt, but recovery becomes possible:

```
switch# cidrecov

CID 1 Non-Critical Seeprom  is Inaccessible or Corrupted.
    CID Non-Critical Seeprom Problem Details
CID 1 Non-Critical Seeprom IP address Control Data Checksum Bad !!!!
CID 1 IP address Control Data:
Version: 0xa
Checksum: 0x0
Size: 0x3
CID 2 IP address Control Data:
Version: 0xa
Checksum: 0x7
Size: 0x3
***WARNING: Recovering IP Data May Affect Both IP  Control and IP Records ***
Backup Current Data Displayed Below If Needed.
CID 1 Chassis Name: VDX8770-4
CID 2 Chassis Name: VDX8770-4
CID 1 IP address Control Data:
Version: 0xa
Checksum: 0x0
Size: 0x3
CID 2 IP address Control Data:
Version: 0xa
Checksum: 0x7
Size: 0x3
IP address Record 1  on CID 1
1st IP Address: 10.17.19.53
1st IP Mask: 255.255.240.0
2nd IP Address: 10.17.19.54
2nd IP Mask: 255.255.240.0
Gateway Address: 10.17.16.1
IP address Record 1  on CID 2
1st IP Address: 10.17.19.53
1st IP Mask: 255.255.240.0
2nd IP Address: 10.17.19.54
2nd IP Mask: 255.255.240.0
Gateway Address: 10.17.16.1
IP address Record 2  on CID 1
1st IP Address: 10.17.19.52
1st IP Mask: 255.255.240.0
2nd IP Address: 0.0.0.0
2nd IP Mask: 0.0.0.0
Gateway Address: 0.0.0.0
IP address Record 2  on CID 2
1st IP Address: 10.17.19.52
1st IP Mask: 255.255.240.0
2nd IP Address: 0.0.0.0
2nd IP Mask: 0.0.0.0
Gateway Address: 0.0.0.0
        CID Recovery Options
0. Exit
1. Recover with default values
2. Recover BAD from GOOD
Enter Selection > 2

Copy IP Data table...
    Copy 384 bytes from CID 2 to CID 1, num blks 1 resid 128
    Read block 1 from CID 2 succeeded
    Write block 1 to CID 1 succeeded
    Read last block from CID 2 succeeded
    Write last block to CID 1 succeeded
    copy successful
Copy succeeded for all data types attempted
IP Address CID Recovery completed.
```

Example 2: Non-critical SEEPROM is inaccessible or corrupt, but recovery is not possible:

```
switch# cidrecov

CID 1 Non-Critical Seeprom  is Inaccessible or Corrupted.
    CID Non-Critical Seeprom Problem Details
CID 1 Non-Critical Seeprom  Read Failed.
Recovery is not possible. Please contact Brocade Technical Support for replacement of the inaccessible
CID(s).
```

Example 3: Critical SEEPROM data is mismatched, recovery is not possible:

```
switch# cidrecov

CID 1 and CID 2 Critical Seeprom Data is Mismatched.
    CID Seeprom Problem Details
CID Seeprom Chassis Serial Number Mismatch.
CID 1 Serial Number: BYP3G15G00N
CID 2 Serial Number: BYP3G17H00P
Recovery is not possible. Please contact Brocade Technical Support for replacement of the corrupted
CID(s).
```

cipherset

Configures FIPS-compliant ciphers for the Lightweight Directory Access Protocol (LDAP) and Secure Shell (SSH) for LDAP and SSH protocols.

Syntax

cipherset { **ldap** | **ssh** | **radius**}

Command Default

There are no restrictions on LDAP and SSH ciphers.

Parameters

radius
: Specifies secure RADIUS ciphers.

ldap
: Specifies secure LDAP ciphers.

ssh
: Specifies secure SSH ciphers.

Modes

Privileged EXEC mode

Usage Guidelines

A switch must be configured with secure ciphers for SSH before that switch can be FIPS compliant. If LDAP authentication is to be used, the LDAP ciphers are also required before a switch can be FIPS compliant.

The secure LDAP ciphers are AES256-SHA, EAS128-SHA, and DES-CBC3-SHA. The secure SSH ciphers are HMAC-SHA1 (mac), 3DES-CBC, AES128-CBC, AES192-CBC, and AES256-CBC.

This command can be entered only from a user account with the admin role assigned.

Examples

To configure secure RADIUS ciphers:

```
switch# cipherset radius

RADIUS cipher list configured successfully
```

To configure secure LDAP ciphers:

```
switch# cipherset ldap

ldap cipher list configured successfully
```

To configure secure SSH ciphers:

```
switch# cipherset ssh

ssh cipher list configured successfully
```

cisco-interoperability

Configures the switch to interoperate with some legacy Cisco switches.

Syntax

cisco-interoperability { **disable** | **enable** }

Command Default

Cisco interoperability is disabled.

Parameters

disable

Disables Cisco interoperability for the Multiple Spanning Tree Protocol (MSTP) switch.

enable

Enables Cisco interoperability for the MSTP switch.

Modes

Protocol Spanning Tree MSTP mode

Usage Guidelines

For some switches, the MSTP field, Version 3 Length, does not adhere to the current standards.

If Cisco interoperability is required on any switch in the network, then all switches in the network must be compatible, and therefore enabled using this command for interoperability with a Cisco switch.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Examples

To enable Cisco interoperability on a switch:

```
switch# configure terminal
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# cisco-interoperability enable
```

To disable Cisco interoperability on a switch:

```
switch# configure terminal
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# cisco-interoperability disable
```

class

Creates a class-map in a policy-map and enters the class-map configuration mode.

Syntax

class *class-mapname*

no class *class-mapname*

Command Default

A policy-map is not created.

Parameters

class-mapname
The designated name for the class-map.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a class-map for a police policy-map with QoS and policing parameters for inbound or outbound traffic. The class-map must have been created and associated with match criteria using the **class-map** command. (Refer to the **qos cos** command.) When you launch the **class** command while in config-policymap mode (refer to **policy-map**) for a policy, the system is placed in "configure policy-map classification" (config-policymap-class) mode. Once this is done you can configure QoS and policing parameters for the class-map using the commands for the specific parameters. The commands that set the parameters for a class-map are:

- **cbs**
- **eir**
- **ebs**
- **conform-set-dscp**
- **conform-set-prec**
- **conform-set-tc**
- **exceed-set-dscp**
- **exceed-set-prec**
- **exceed-set-dscp**
- **police cir**
- **set-priority**

The QoS and policing parameters define the cir, cbs, ebr, and eir rates and the actions that must occur when traffic conforms or exceeds designated rates. For more details on these parameters, refer to the "Port-based Policer" section in the "QoS Configuration" chapter of the *Network OS Administrator's Guide*. Each policy-map can contain one class-map.

Enter the **no policy-map***name* command to remove the policy-map. Associate the policy-map to the interface for inbound or outbound direction with the **service-policy** command (refer to **service-policy**).

Enter **no police** while in config-policymap-class mode to remove all policing parameters for the class-map.

Enter **no police** command followed by a policing parameter name to remove a specific parameter.

NOTE
The **cir** and **cbs** parameters are the mandatory for configuring a class-map. Other parameters are optional. If optional parameters are not set then they will be treated as disabled. To delete the mandatory cir or cbs parameters, you must delete all Policer parameters while in the policy-map class configuration mode using the **no police** command.

NOTE
This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# cbs 50000
switch(config-policymap-class-police)# eir 800000
switch(config-policymap-class-police)# ebs 400000
switch(config-policymap-class-police)# conform-set-tc 3
switch(config-policymap-class-police)# exceed-set-prec 4
```

class-map

Enters class-map configuration mode.

Syntax

class-map *class-map-name*

no class-map *class-map-name*

Command Default

The class-name "class-default" is reserved and cannot be created by users.

Parameters

class-map-name

Name of classification map. The map name is restricted to 64 characters.

Modes

Global configuration mode

Usage Guidelines

Enter **no map class-map***class-map-name* while in global configuration mode to remove the classification map.

Only 128 class maps are allowed.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a classification map and place system into config-classmap mode:

```
switch(config)# class-map default

switch(config-classmap)#
```

NOTE

The class map created using **class map** becomes the default class-map and cannot be removed using the **no class-map** command. You can remove a class-map from a policy map however.

clear ag nport-utilization

Clears Access Gateway N_Port utilization information.

Syntax

clear ag nport-utilization [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

You can clear N_Port utilization information either for a specific RBridge or for all.

rbridge-id

Specify an RBridge ID.

all

Clear N_Port utilization information for N_Ports on all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Enabling a port also clears the information

There is a **show** form of this command, which shows Access Gateway N_Port utilization information.

Examples

The following command clears utilization information for Access Gateway N_Ports on RBridge 1:

```
switch# clear ag nport-utilization rbridge-ID 1
```

The following command clears Access Gateway utilization information for all N_Ports on the switch:

```
switch# clear ag nport-utilization rbridge-ID all
```

History

Release version	Command history
5.0.0	This command was introduced.

clear arp

Clears the ARP statistics cache on the host.

Syntax

clear arp [<*N*>**gigabitethernet** *rbridge-id/slot/port* [**no-refresh**] | [**ip** *ip-address* [**no-refresh**] [**vrf** {*vrf-name* | **all** }] | [**rbridge-id** { *rbridge-id* | **all** }] | [**no-refresh** [**vrf** { *vrf-name* | **all** }] [**rbridge-id** { *rbridge-id* | **all** }] | [**rbridge-id** { *rbridge-id* | **all** }] | [**vrf** {*vrf_name* | **all** }] [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

no-refresh

Deletes the ARP entries.

ip

Clears the statistics on all interfaces.

ip-address

Clears the ARP for this next-hop IP address.

no-refresh

Deletes the ARP entries.

vrf

Specifies a VRF instance or all instances.

vrf_name

Specifies a VRF instance.

all

Specifies all VRF instances.

Modes

Privileged EXEC mode

clear counters

Clears the IP counter statistics on the switch.

Syntax

clear counters [**access-list** { **ip** | **ipv6** | **mac** } [**all** | **interface** { **fcoe** [*vn-number* | **all**] | **port-channel** *number* | **fibrechannel** *rbridge-id/slot/port* |<*N*>**gigabitethernet** *rbridge-id/slot/port* } | **slot-id** *number* | **vlan** *vlan_id* } | **storm-control**]

Parameters

access-list
Clears the IP counter statistics on all interfaces on the switch.

all
Clears all IP counter statistics on the switch or selected interface.

interface
Specifies an interface.

port-channel *number*
Specifies a port-channel. The number of available channels range from 1 through 6144.

<*N*>**gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

vlan *vlan_id*
Specifies the VLAN interface to which the ACL is bound.

slot-id
Clears the IP counter statistics on a specified slot in the chassis.

storm-control
Clears counters about traffic controlled by configured rate limits.

Modes

Privileged EXEC mode

clear counters (IP)

Clears the IP counter statistics on all interfaces on the switch.

Syntax

clear counters { **all** | **access-list ip** *access_list_name* | **interface** { **port-channel** *number* | **fibrechannel** { *rbridge-id/slot/port* } | *<N>*__gigabitethernet__ { *rbridge-id/slot/port* } | **slot-id** *number* | **ve** *vlan_id* } { **in** | **out** }

Parameters

all

Clears statistics on all interfaces.

access-list ip *access_list_name*

Specifies the name of the IP access list.

in | **out**

Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.

interface

Specifies n interface.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

fibrechannel *rbridge-id/slot/port*

Specifies a valid Fibre Channel interface.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

slot-id *number*

Specifies the slot number of the linecard.

ve *vlan_id*

Specifies the virtual Ethernet (VE) interface to which the ACL is bound. (Refer to the Usage Guidelines.)

rbridge-id

Specifies RBridge ID for node-specific ACL interface details.

rbridge-id | **all**

Specifies the unique identifier for a switch. All refers to all rbridge-ids in the cluster.

Modes

Privileged EXEC mode

Usage Guidelines

The **clear counters all** command does not clear counters for any of the protocol daemon stats like LLDP, LACP, MSTP, and so on.

For Brocade VDX switches, the slot number is always 0 (zero).

Examples

To clear the statistics for the 10-gigabit Ethernet interface 5/0/1:

```
switch# clear counters interface tengigabitethernet 5/0/1
```

To clear the statistics for all the interfaces on the linecard in slot 0 (zero):

```
switch# clear counters slot-id 0
```

Related Commands

show ip igmp groups

clear counters (MAC)

Clears the MAC counter statistics on all interfaces on the switch.

Syntax

clear counters { **all** | **access-list mac** *access_list_name* | **interface** { **port-channel** *number* } | **fibrechannel** { *rbridge-id/slot/port* } | <*N*>**gigabitethernet** { *rbridge-id/slot/port* } | **slot-id** *number* | **vlan** *vlan_id* }

Parameters

all

Clears statistics on all interfaces.

access-list mac *access_list_name*

Specifies the name of the MAC access list.

in|**out**

Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.

interface

Specifies the use of the *port-channel* , *fibrechannel* , *gigabitethernet* or *tengigabitethernet* keyword.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

fibrechannel *rbridge-id/slot/port*

Specifies a valid Fibre Channel interface.

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

vlan *vlan_id*

Specifies the VLAN interface to which the ACL is bound. (Refer to the Usage Guidelines.)

slot-id *number*

Specifies the slot number of the linecard.

Modes

Privileged EXEC mode

Usage Guidelines

The **clear counters all** command does not clear counters for any of the protocol daemon stats like LLDP, LACP, MSTP, and so on.

For Brocade VDX switches, the slot number is always 0 (zero).

Examples

To clear the statistics for the 10-gigabit Ethernet interface 5/0/1:

```
switch# clear counters interface tengigabitethernet 5/0/1
```

To clear the statistics for all the interfaces on the linecard in slot 0 zero):

```
switch# clear counters slot-id 0
```

Related Commands

show ip igmp groups

clear counters access-list

For a given network protocol and inbound/outbound direction, clears ACL statistical information. You can clear all statistics for a specified ACL or only for that ACL on a specified interface. You can also clear statistical information for all ACLs bound to a specified switch interface, VLAN, VE, or VXLAN overlay gateway.

Syntax

clear counters access-list [{**ip** | **ipv6** | **mac** *name*} {**interface** *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* | **all**} {**in** | **out** }]

Parameters

ip | **ipv6** | **mac**
Specifies the network protocol.

name
Specifies the ACL name. To clear statistics on all counters of an ACL-type, do not specify *name*.

interface
Filter by interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge_id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel. Available channels range from 1 through 6144.

vlan *vlan_id*
(Available only on Layer 2) Specifies a VLAN.

ve *vlan_id*
(Available only on Layer 3) Specifies a virtual Ethernet (VE) interface.

rbridge-id
(for a VE interface) To display ACLs beyond the local node, include this keyword and the relevant of the following:

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

overlay-gateway *overlay_gateway_name*
Specifies a VXLAN overlay-gateway.

in | **out**
Specifies the binding direction (incoming or outgoing).

Modes

Privileged EXEC mode

Examples

The following example clears ACL statistics for the 10-gigabit Ethernet interface 5/0/1:

```
switch# clear counters access-list interface tengigabitethernet 5/0/1
```

The following example clears counters for the configured MAC access list named test on an interface:

```
switch# clear counters access-list mac test interface tengigabitethernet 5/0/1
```

The following example clears counters for the configured MAC access list named test on all interfaces on which this ACL is applied:

```
switch# clear counters access-list mac test
```

The following example clears counters for the configured IPv4 access list named test on an interface:

```
switch# clear counters access-list ip test interface tengigabitethernet 6/0/1
```

The following example clears counters for the configured IPv4 access list named test on all interfaces on which this ACL is applied:

```
switch# clear counters access-list ip test
```

The following example clears the incoming statistics for an IPv6 ACL on RBridge 122 on a virtual Ethernet (VE) interface:

```
switch# clear counters access-list ipv6 ip_acl_3 interface ve 10 in rbridge-id 122
```

The following example clears the (incoming) statistics for all ACLs applied to a specified overlay gateway:

```
switch# clear counters access-list overlay-gateway gw121 in
```

clear counters interface

Clears the IP counter statistics on a specified interface on the switch.

Syntax

clear counters interface { **fcoe** { *vn-number/rbridge-id/port* | **all** } | **fibrechannel** { *rbridge-id/slot/port* } | **port-channel** *number* | [*<N>*__gigabitethernet__ { *rbridge-id/slot/port* | **all** }] | **vlan** { *vlan_id* } }

Parameters

interface

Specifies the use of the *fcoe, port-channel* , *fibrechannel* , *fortygigabitethernet* , *gigabitethernet, tengigabitethernet,* or *vlan* keyword.

fcoe*vn-number/rbridge-id/port*

Specifies the FCOE interface name.

vn-number

Specifies the VN number for FCoE.

rbridge-id

Specifies the RBridge ID.

port

Specifies a valid port number.

all

Clears counters for all FCoE interfaces.

fibrechannel*rbridge-id/slot/port*

Specifies a valid Fibre Channel interface.

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

vlan *vlan_id*
Specifies a VLAN interface. (Refer to the Usage Guidelines.)

Modes

Privileged EXEC mode

Usage Guidelines

The **clear counters all** command does not clear counters for any of the protocol daemon stats such as LLDP, LACP, MSTP, and so on.

For Brocade VDX switches, the slot number is always 0 (zero).

clear counters slot-id

Clears the IP counter statistics on a specified slot in the chassis.

Syntax

clear counters slot-id *num*

Parameters

num

Specifies a valid integer.

Modes

Privileged EXEC mode

Usage Guidelines

The **clear counters all** command does not clear counters for any of the protocol daemon statistics such as LLDP, LACP, MSTP, and so on.

For Brocade VDX switches, the slot number is always 0 (zero).

clear counters storm-control

Clears counters related to traffic controlled by configured rate limits.

Syntax

clear counters storm-control

clear counters storm-control broadcast [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port*]

clear counters storm-control interface { *<N>***gigabitethernet** *rbridge-id/slot/port* }

clear counters storm-control multicast [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* }

clear counters storm-control unknown-unicast [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* }

Parameters

clear counters storm-control
Clears all BUM (Broadcast, Unknown unicast and Multicast)-related counters in the system.

clear counters storm-control broadcast
Clears all BUM-related counters in the system for the broadcast traffic type.

clear counters storm-control interface *type rbridge-id/slot/port*
Clears all BUM-related counters in the system for the specified interface. You must specify an interface type, followed by the RBridge ID/slot/port.

show storm-control multicast
Clears all BUM-related counters in the system for the multicast traffic type.

clear counters storm-control unknown-unicast
Clears all BUM-related counters in the system for the unknown-unicast traffic type.

interface *<N>***gigabitethernet** *rbridge-id/slot/port*
Specifies an interface type, followed by the RBridge ID/slot/port, for which to clear all BUM-related counters in the system for the specified traffic type. Use this parameter to clear counters on a per-port basis.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N* **gigabitethernet** *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears the counters for Broadcast, Unicast, and unknown-Multicast (BUM) traffic for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

Examples

To clear counters for broadcast traffic on the 10-gigabit Ethernet interface 102/4/1:

```
switch# clear counters storm-control broadcast interface tengigabitethernet 102/4/1
```

To clear counters for all traffic types enabled on the 10-gigabit Ethernet interface 102/4/1:

```
switch# clear counters storm-control interface tengigabitethernet 102/4/1
```

To clear counters for all multicast traffic in the system:

```
switch# clear counters storm-control multicast
```

To clears all BUM-related counters in the system:

```
switch# clear counters storm-control
```

clear dot1x statistics

Clears all accumulated dot1x port authentication statistics on all ports.

Syntax

clear dot1x statistics

Modes

Privileged EXEC mode

Examples

To clear dot1x statistics:

```
switch# clear dot1x statistics
```

Related Commands

clear dot1x statistics interface

clear dot1x statistics interface

Clears all dot1x statistics for a specified interface port.

Syntax

clear dot1x statistics interface [*<N>*gigabitethernet *rbridge-id/slot/port*]

Parameters

*<N>*gigabitethernet

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N*gigabitethernet with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To clear dot1x statistics on a port:

```
switch# clear dot1x statistics interface tengigabitethernet 0/16
```

Related Commands

clear dot1x statistics

clear edge-loop-detection

Re-enables all ports disabled by ELD and clears all ELD statistics.

Syntax

clear edge-loop-detection [**rbridge-id** *rbridge-id*]

clear edge-loop-detection interface { *<N>*__gigabitethernet__ { *rbridge-id/slot/port* } | **port-channel** *num* }

Parameters

rbridge-id

A unique identifier for the switch. Values are from 1 through 239.

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *num*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

Modes

ELD configuration mode

Usage Guidelines

This operation is typically performed after correcting a configuration error that caused ELD to disable ports.

This command applies to Brocade VCS Fabric mode only.

This functionality detects Layer 2 loops only.

If the rbridge-id is specified, it clears edge-loop-detection from the specific node. Otherwise, it clears edge-loop-detection from all nodes in the VCS cluster.

Related Commands

protocol edge-loop-detection, show edge-loop-detection rbridge-id, show edge-loop-detection interface

clear fcoe login

Clears the FCoE login for a given FCoE interface, VLAN, virtual fabric ID, or device World Wide Name (WWN).

Syntax

clear fcoe login [**interface fcoe** *vn-number/rbridge-id/front-port-number*] | [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port*] | [**port-channel** *port-channel-num*] [**vlan** *vlan_id*] | [**vfid** *vfid*] | [**device** *device-wwn*]

Parameters

interface fcoe *vn-number/rbridge-id/front-port-number*

Specifies a virtual network number, as well as an RBridge ID and front port number for the virtual fabric. The value for *vn-number* is 1. The *front-port-number* is a logical FCoE port number in the RBridge ID.

vlan *vlan_id*

Specifies a VLAN ID for the device.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel.

vfid *vfid*

Specifies the virtual fabric ID for the device.

device *device-wwn*

Specifies the WWN of the device.

Modes

Privileged EXEC mode

Examples

```
switch# clear fcoe login interface fcoe 1/1/1
switch# clear fcoe login device 10:00:00:05:1e:8e:be:40
switch# clear fcoe login interface tengigabitethernet 1/0/1
switch# clear fcoe login vlan 1002
switch# clear fcoe login vfid 1
```

clear ip bgp dampening

Reactivates all suppressed BGP4 routes.

Syntax

clear ip bgp dampening [*ip-addr* { **/** *mask* }]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

To unsuppress all suppressed BGP4 routes:

```
switch# clear ip bgp dampening
```

clear ip bgp flap-statistics

Clears the dampening statistics for a BGP4 route without changing the dampening status of the route.

Syntax

clear ip bgp flap-statistics [*ip-addr* { **/** *mask* } | **neighbor** *ip-addr* | **regular-expression** *string*]

Parameters

ip-addr
: IPv4 address of a specified route in dotted-decimal notation.

mask
: (Optional) IPv4 mask of a specified route in CIDR notation.

neighbor
: Clears dampening statistics only for routes learned from the specified neighbor.

  ip-addr
  : IPv4 address of the neighbor.

regular-expression
: Specifies a regular expression.

  string
  : Regular expression.

Modes

Privileged EXEC mode

Examples

To clear the dampening statistics for a BGP4 route:

```
switch# clear ip bgp flap-statistics 10.0.0.0/16
```

clear ip bgp local routes

Clears all BGP4 local routes from the IP route table and resets the routes.

Syntax

clear ip bgp local routes

Modes

Privileged EXEC mode

Examples

To clear all BGP4 local routes:

```
switch# clear ip bgp local routes
```

clear ip bgp neighbor

Requests a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Syntax

clear ip bgp neighbor [**all** | *as-num* | *peer-group-name* | *ip-addr*] [**last-packet-with-error** | **notification-errors** | **soft** [**in** | **out**] | **soft-outbound** | **traffic**] [**rbridge-id** *rbridge-id*]

Parameters

all
Resets and clears all BGP4 connections to all neighbors.

as-num
Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name
Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.

ip-addr
Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.

last-packet-with-error
Clears all BGP4 connections identified as having the last packet received with an error.

notification-errors
Clears all BGP4 connections identified as having notification errors.

soft
Refreshes routes received from or sent to the neighbor.

in
Refreshes received routes.

out
Refreshes sent routes.

soft-outbound
Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic
Clears the counters (resets them to 0) for BGP4 messages.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To refresh all BGP4 neighbor connections:

```
switch# clear ip bgp neighbor all
```

clear ip bgp routes

Clears BGP4 routes from the IP route table and resets the routes.

Syntax

clear ip bgp routes [*ip-addr* { **/** *mask* }]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

To clear BGP4 routes:

```
switch# clear ip bgp routes 10.0.0.0/16
```

clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

Syntax

clear ip bgp traffic

Modes

Privileged EXEC mode

Examples

To clear the BGP4 message counters:

```
switch# clear ip bgp traffic
```

clear ip dhcp relay statistics

Clears IP DHCP Relay statistics

Syntax

clear ip dhcp relay statistics

clear ip dhcp relay statistics ip-address *ip-address*

clear ip dhcp relay statistics [**ip-address** *ip-address*] **rbridge-id** { *rbridge-id* | **all** | **range** }

Command Default

DHCP Relay statistics are present on the DHCP server.

Parameters

ip-address *ip-address*

IPv4 address of DHCP server where client requests are to be forwarded.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

range

Specifies multiple RBridge IDs. You can specify a range (for example, 3-5), a comma-separated list (for example, 1, 3, 5. 6), or you can combine a range with a list (for example, 1-5, 6, 8).

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clears IP DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on a local switch, specific switches, or all nodes in a logical chassis cluster.

If the **rbridge-id** parameter is omitted, statistics are cleared for the local switch. If the **ip_address** parameter is omitted, statistics cleared for all configured addresses on defined switches.

No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster.

Examples

The following example clears statistics for IP DHCP Relay addresses on RBridge IDs 1, 3, and 5.

```
switch# clear ip dhcp relay statistics rbridge-id 1,3,5
```

The following example clears statistics for IP DHCP Relay address 10.1.0.1 configured on RBridge IDs 1, 3, and 5.

```
switch# clear ip dhcp relay statistics ip-address 10.1.0.1 rbridge-id 1,3,5
```

Related Commands

show ip dhcp relay statistics

clear ip fabric-virtual-gateway

Clears IP Fabric-Virtual-Gateway protocol statistics globally or for a Virtual Ethernet (VE) interface.

Syntax

clear ip fabric-virtual-gateway { **all** | **interface ve** *vlan-id* }

Command Default

None

Parameters

all

Retriggers the election of ARP responders for all sessions.

interface ve *vlan-id*

Clears IP Fabric-Virtual-Gateway configurations for the specified VE interface. The range is from 1 through 8191.

Modes

Privileged EXEC mode

Usage Guidelines

A **clear** command must be issued to retrigger the election of a new ARP responder.

Examples

The following example clears the IP Fabric-Virtual-Gateway protocol globally.

```
switch# clear ip fabric-virtual-gateway all
```

The following example clears the IP Fabric-Virtual-Gateway protocol for a specific VE interface.

```
switch# clear ip fabric-virtual-gateway interface ve 2000
```

History

Release version	Command history
5.0.1	This command was introduced.

clear ip igmp groups

Clears information related to learned groups in the IGMP module.

Syntax

clear ip igmp groups [*A.B.C.D*] [**interface** { **port-channel** *number* | **vlan** *vlan_id* } | *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **vlan** *vlan_id* | **ve** *vlan_id* }] [**rbridge** *rbridge-id*]

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

interface

Specifies an interface.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel. The number of available channels range from 1 through 6144.

vlan *vlan_id*

Specifies a VLAN. Refer to "Usage Guidelines" below.

ve *vlan_id*

Specifies groups on the specified virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)

rbridge *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To clear information for all groups in the IGMP protocol:

```
switch# clear ip igmp groups
```

clear ip igmp statistics interface

Clears statistical information related to the IGMP database.

Syntax

clear ip igmp statistics interface { *<N>*__gigabitethernet__ *rbridge-id/slot/port* | **port-channel** *number* | **ve** *vlan_id* | **vlan** *vlan_id* [**rbridge** *rbridge-id*] | **rbridge** *rbridge-id* }

Parameters

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)

vlan *vlan_id*

Specifies a VLAN interface. (Refer to the Usage Guidelines.)

rbridge *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command can be used with User-configurable VLAN IDs.

In logical chassis mode:

- When the **rbridge-id** option is specified, details for the ve interface on that particular rbridge are cleared.
- If **rbridge-id** is not specified, details for the ve interface on the node on which the command is executed are cleared.
- When **rbridge-idall** is specified, all ve interfaces with that **rbridge-id** from all the nodes in the cluster are cleared.

Examples

To clear statistics information for a VLAN in the IGMP protocol:

```
switch# clear ip igmp statistics interface vlan 11
```

clear ip ospf

Clears OSPF process, counters, neighbors, or routes.

Syntax

clear ip ospf all

clear ip ospf counters { **all** | *<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id* } }
[**vrf** *name* [**rbridge** *rbridge-id*]] | [**rbridge-id** *rbridge-id*]

clear ip ospf neighbor { *A.B.C.D* | **all** }

clear ip ospf routes { *A.B.C.D* | **all** }

Parameters

all
Clears all counters.

counters
Clears all counters or clears the counters of an interface that you specify.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

loopback *number*
Specifies a loopback port number in the range of 1 to 255.

port-channel *number*
Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)

rbridge *rbridge-id*
Specifies an RBridge ID.

vrf *name*
Clears the specified VRF.

neighbor
Clears the specified neighbor, or clears all neighbors.

A.B.C.D
Specifies the IP address of the neighbor to clear.

all

Clears all neighbors.

routes

Clears matching routes or clears all routes.

A.B.C.D

Clears all routes that match the prefix and mask that you specify.

all

Clears all routes.

Modes

Privileged EXEC mode

Usage Guidelines

If the physical interface type and name are specified, the **rbridge-id***rbridge-id* option is not available.

Examples

To restart the OSPF processes:

```
switch# clear ip ospf all
```

clear ip pim mcache

Clears the Protocol Independent Multicast forwarding cache.

Syntax

clear ip pim mcache [*IP-addr* [*IP-addr*]]

Parameters

IP-addr

Group or source IPv4 address. One or two IP addresses (unicast or multicast) can be specified.

Modes

Privileged EXEC mode

Related Commands

clear ip pim rp-map, clear ip pim traffic

clear ip pim rp-map

Clears the static multicast forwarding table.

Syntax

clear ip pim rp-map

Modes

Privileged EXEC mode

Usage Guidelines

This command should be used after the static Rendezvous Point configuration has been changed. This allows Protocol Independent Multicast to immediately start using the new Rendezvous Point, rather than waiting for the old information to expire.

Related Commands

clear ip pim mcache, clear ip pim traffic

clear ip pim traffic

Clears the Protocol Independent Multicast (PIM) traffic counters.

Syntax

clear ip pim traffic

Modes

Privileged EXEC mode

Related Commands

clear ip pim rp-map, clear ip pim mcache

clear ip route

Clears a specified route or all IP routes in the IP routing tables.

Syntax

clear ip route { *A.B.C.D/M* | **all** | **slot** *line_card_number* | **vrf** *name* }

Parameters

A.B.C.D/M
Clears the route specified by this IPv4 address/length.

all
Clears all routes from the routing table in IP route management.

slot *line_card_number*
Clears the route specified by this line card number.

vrf *name*
Clears the specified VRF.

Modes

Privileged EXEC mode

Examples

To clear the IP route specified by the prefix 192.158.1.1/24:

```
switch# clear ip route 192.158.1.1/24
```

clear ipv6 bgp dampening

Reactivates all suppressed BGP4+ routes.

Syntax

clear ipv6 bgp dampening [*ipv6-addr* { **/** *mask* }]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv6 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

To unsuppress all suppressed BGP4+ routes:

```
device# clear ipv6 bgp dampening
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 bgp flap-statistics

Reactivates all suppressed BGP4+ routes.

Syntax

clear ipv6 bgp flap-statistics [*ipv6-addr* { **/** *mask* } | **neighbor** *ipv6-addr* | **regular-expression** *string*]

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv6 mask of a specified route in CIDR notation.

neighbor
Clears dampening statistics only for routes learned from the specified neighbor.

ipv6-addr
IPv6 address of the neighbor.

regular-expression
Specifies a regular expression.

string
Regular expression.

Modes

Privileged EXEC mode

Examples

To clear the dampening statistics for a BGP4+ route:

```
device# clear ipv6 bgp flap-statistics
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 bgp local routes

Clears all BGP4+ local routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp local routes

Modes

Privileged EXEC mode

Examples

To clear all BGP4+ local routes:

```
device# clear ipv6 bgp local routes
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 bgp neighbor

Requests a dynamic refresh of BGP4+ connections or routes from a neighbor, with a variety of options.

Syntax

clear ipv6 bgp neighbor [**all** | *as-num* | *peer-group-name* | *ipv6-addr*] [**last-packet-with-error** | **notification-errors** | **soft** [**in** | **out**] | **soft-outbound** | **traffic**] [**rbridge-id** *rbridge-id*]

Parameters

all
Resets and clears all BGP4+ connections to all neighbors.

as-num
Clears all BGP4+ connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name
Clears all BGP4+ connections in this peer group. Range is from 1 through 63 characters.

ipv6-addr
Clears all BGP4+ connections with this IPv6 address, in dotted-decimal notation.

last-packet-with-error
Clears all BGP4+ connections identified as having the last packet received with an error.

notification-errors
Clears all BGP4+ connections identified as having notification errors.

soft
Refreshes routes received from or sent to the neighbor.

in
Refreshes received routes.

out
Refreshes sent routes.

soft-outbound
Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4+ route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic
Clears the counters (resets them to 0) for BGP4+ messages.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To refresh all BGP4 neighbor connections:

```
device# clear ipv6 bgp neighbor all
```

To reset the counters for BGP4+ messages:

```
device# clear ipv6 bgp neighbor all traffic
```

To clear all BGP4+ connections with a specified IPv6 address:

```
device# clear ipv6 bgp neighbor 2001::1
```

To clear all BGP4+ connections with a specified peer group:

```
device# clear ipv6 bgp neighbor P1
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 bgp routes

Clears BGP4+ routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp routes [*ipv6-addr* { **/** *mask* }]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv6 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

To clear BGP4+ routes:

```
device# clear ipv6 bgp routes 2000::/64
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 bgp traffic

Clears the BGP4+ message counter for all neighbors.

Syntax

clear ipv6 bgp traffic

Modes

Privileged EXEC mode

Examples

To clear the BGP4+ message counters:

```
device# clear ipv6 bgp traffic
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 counters

Clears IPv6 counters on on all interfaces or on a specified interface.

Syntax

clear ipv6 counters [**all** | **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** *port_number* | **ve** *vlan_id* [**rbridge-id** [**all** | *rbridge-id*] }]

Parameters

all

Specifies all interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback

Specifies a loopback interface.

port_number

Port number of the loopback interface.The range is from 1 through 255.

ve

Specifies a virtual Ethernet (VE) interface.

vlan_id

VLAN ID of the VE interface.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

all

Specifies all RBridges in the cluster.

Modes

Privileged EXEC mode

clear ipv6 dhcp relay statistics

Clears IPv6 DHCP Relay statistics

Syntax

clear ipv6 dhcp relay statistics [**ipv6-address** *ipv6-address*] [**rbridge-id** { *rbridge-id* | **all** } | **range**]

Command Default

If the **rbridge-id** parameter is omitted, statistics clear for the local switch. If the **ip_address** parameter is omitted, statistics clear for all configured addresses on defined switches.

Parameters

ip-address *ip-addr*

IPv6 address of DHCP server where client requests are to be forwarded.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

range

A range of RBridge IDs separated by a dash or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

Clears IPv6 DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on a local switch, specific switches, or all nodes in a logical chassis cluster.

No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster.

Examples

Clear statistics for IPv6 DHCP Relay addresses on RBridge IDs 1, 3, and 5.

```
switch# clear ipv6 dhcp relay statistics rbridge-id 1,3,5
```

History

Release version	Command history
5.0.1	This command was introduced.

clear ipv6 fabric-virtual-gateway

Clears IPv6 Fabric-Virtual-Gateway protocol statistics globally or for a Virtual Ethernet (VE) interface.

Syntax

clear ipv6 fabric-virtual-gateway { **all** | **interface ve** *vlan-id* }

Command Default

None

Parameters

all Specifies all statistics.

interface ve ***vlan-id*** Clears IPv6 Fabric-Virtual-Gateway configurations for the specified VE interface. The range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

Modes

Privileged EXEC mode

Usage Guidelines

None

Examples

Clears the IPv6 Fabric-Virtual-Gateway protocol statistics on VE 2000.

```
switch# clear ipv6 fabric-virtual-gateway interface ve 2000
```

History

Release version	Command history
5.0.1	This command was introduced.

clear ipv6 mld groups

Clears IPv6 MLDv1 group cache entries for a multicast group address or a VLAN.

Syntax

clear ipv6 mld groups [*ipv6address*] [**interface vlan** *vlan_id*]

Parameters

ipv6address
: Specifies the IPv6 address for the group.

interface vlan
: Specifies a VLAN ID.

vlan_id
: A VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

Modes

Privileged EXEC mode

Examples

To clear all IPv6 MLDv1 group cache entries:

```
switch# clear ipv6 mld groups
```

To clear IPv6 MLDv1 group cache entries on a sp[ecific VLAN:

```
switch# clear ipv6 mld groups interface vlan 2000
```

clear ipv6 mld statistics

Clears IPv6 MLDv1 snooping statistics for a VLAN.

Syntax

clear ipv6 mld statistics [**interface vlan** *vlan_id*]

Parameters

interface vlan

Specifies a VLAN ID.

vlan_id

A VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

Modes

Privileged EXEC mode

Examples

To clear IPv6 MLDv1 snooping statistics for a specific VLAN:

```
switch# clear ipv6 mld statistics interface vlan 2000
```

clear ipv6 neighbor

Clears the IPv6 Neighbor Discovery cache on an interface.

Syntax

clear ipv6 neighbor [*ipv6address*] [**force-delete** [**rbridge-id** *rbridge-id*] | **interface** [*<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id*] | **no-refresh** [**rbridge-id** *rbridge-id*] | **slot** *slot* | **ve** *vlan_id* | **vrf** [*vrf-name* | **all** | **default-vrf**] [**force-delete** | **no-refresh**] [**rbridge-id** *rbridge-id*]]

Parameters

ipv6address
IPv6 address of a neighbor in *A:B::C:D* format.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

force-delete
Forcibly clears the cache.

no-refresh
Prevents the cache from being refreshed.

slot
Specifies a slot.

slot
Line card number.

ve
Specifies a virtual Ethernet (VE) interface.

vlan_id
VLAN ID of the VE interface. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

clear ipv6 ospf

Clears OSPFv3 data processes, counts, force-spf, neighbors, redistribution, routes, and traffic.

Syntax

clear ipv6 ospf { **all** | **force-spf** | **redistribution** | **traffic** } [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

clear ipv6 ospf counts neighbor { *A.B.C.D* [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*] } | **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port*] } | [**loopback** *number* | **ve vlan_id** *number* [*A.B.C.D* | **rbridge-id** *rbridge-id*]] }

clear ipv6 ospf neighbor { **all** [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*] } | { **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* } } | [**loopback** *number* | **ve vlan_id** *number* [*A.B.C.D* | **rbridge-id** *rbridge-id*]] }

clear ipv6 ospf routes { *IPv6addr* | **all** } | [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Command Default

OSPFv3 properties are cleared for the default VRF if the VRF is not specified.

Parameters

all
Clears all OSPFv3 data.

force-spf
Performs the shortest path first (SPF) calculation without clearing the OSPFv3 database.

redistribution
Clears OSPFv3 redistributed routes.

traffic
Clears OSPFv3 traffic statistics.

all-vrfs
Specifies all VRFs.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge. Applicable only in case of loopback and ve interfaces.

counts
Clears OSPFv3 counters.

neighbor
Clears all OSPF counters for a specified neighbor.

A.B.C.D
Specifies a destination IPv6 address.

interface
Specifies an interface.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *number*

Specifies a loopback port number in the range from1 through 255.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Refer to the Usage Guidelines.

neighbor

Clears OSPFv3 neighbors.

routes

Clears OSPFv3 routes.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **force-spf** keyword to perform the shortest path first (SPF) calculation without clearing the OSPFv3 database.

If the physical interface type and name are specified, the **rbridge-id***rbridge-id* option is not available.

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples

To restart the OSPFv3 processes:

```
device# clear ipv6 ospf all
```

The following example clears all OSPFv3 counters for a specified neighbor:

```
device# clear ipv6 ospf counts neighbor 10.10.10.1
```

History

Release version	Command history
5.0.0	This command was introduced.

clear ipv6 route

Clears IPv6 routing tables on an interface or line card and reloads the current information.

Syntax

clear ipv6 route [**all** | **slot** *slot* [*ipv6address* | *ipv6prefix*] [**rbridge-id** { **all** | *rbridge-id* } | **vrf** *vrf-name*]]]

Parameters

all
Clears all IPv6 routes.

slot
Clears IPv6 routes on the specified line card.

slot
Slot number.

ipv6address
IPv6 address.

ipv6prefix
IPv6 prefix in *A:B::C:D/length* format.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

all
Specifies all RBridges in the cluster.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

clear ipv6 vrrp statistics

Clears IPv6 VRRPv3 session statistics for all virtual groups, for a specified interface or RBridge ID, or for a specified virtual group.

Syntax

clear ipv6 vrrp statistics [**all**] [**session** *VRID* | **all**] [**rbridge** { *rbridge-id* | **all** }]

clear ipv6 vrrp statistics [**interface** { *<N>***gigabitethernet** [*rbridge-id*]*/slot/port* | **ve** *vlan_id*}]

Parameters

all
Clears all IPv6 VRRP statistics.

session *VRID*
Specifies the virtual group ID on which to clear statistics. Valid values range from 1 through 128.

rbridge-id { *rbridge-id* | **all** }
Clears all IPv6 VRRP statistics for the specified RBridge ID. If **all** is specified for the *rbridge-id* variable, information for all RBridge IDs is displayed.

interface
Specifies an interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an optional RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve *vlan_id*
Specifies the VE VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported in IPv6 VRRPv3 and VRRP-E-v3.

Examples

To clear all IPv6 VRRPv3 statistics for all virtual groups:

```
switch# clear ipv6 vrrp statistics all
```

To clear statistics for an IPv6 VRRPv3 session of a virtual group named 25.

```
switch# clear ipv6 vrrp statistics session 25
```

clear lacp

Clears the Link Aggregation Group Control Protocol (LACP) counters on a specific port-channel.

Syntax

clear lacp *number* **counters**

Parameters

number

Specifies the port channel-group number. Valid values range from 1 through 6144.

counters

Clears traffic counters.

Modes

Privileged EXEC mode

Examples

To clear the LACP counters for a specific port-channel:

```
switch# clear lacp 10 counters
```

Related Commands

show lacp

clear lacp counters

Clears the Link Aggregation Group Control Protocol (LACP) counters on all port-channels.

Syntax

clear lacp counters

Modes

Privileged EXEC mode

Examples

To clear the counters for all port-channels:

```
switch# clear lacp counters
```

Related Commands

show lacp

clear lldp neighbors

Clears the Link Layer Discovery Protocol (LLDP) neighbor information on all or specified interfaces.

Syntax

clear lldp neighbors interface [<*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

interface

Use this parameter followed by the slot or port number to identify the interface.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears the LLDP neighbor information received on all the interfaces.

Examples

To clear the LLDP neighbor information for all interfaces:

```
switch# clear lldp neighbors
```

Related Commands

show lldp neighbors

clear lldp statistics

Clears LLDP statistics for all interfaces or a specified interface.

Syntax

clear lldp statistics interface [*<N>*gigabitethernet *rbridge-id/slot/port*]

Parameters

interface

Use this parameter followed by the slot or port number to identify the interface.

*<N>*gigabitethernet

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N*gigabitethernet with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears all the LLDP statistics on all interfaces.

Examples

To clear all the LLDP statistics for all interfaces:

```
switch# clear lldp statistics
```

Related Commands

show lldp statistics

clear logging auditlog

Clears the audit log system messages.

Syntax

clear logging auditlog [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

This command is executed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To clear the audit log messages on the local switch:

```
switch# clear logging auditlog
```

Related Commands

clear logging raslog, log-dampening-debug, show logging auditlog

clear logging raslog

Clears RASLog messages from the switch.

Syntax

clear logging raslog [**message-type** { **DCE** | **SYSTEM** }] [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

Clear all RASLog messages on the local switch.

Parameters

message-type

Clears RASLog messages of the specified type.

SYSTEM

Clears system messages.

DCE

Clears DCE application messages.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

The **rbridge-id** operand is supported in VCS mode only.

This command is not supported on the standby management module.

Examples

To clear all RASLog messages on the local switch:

```
switch# clear logging raslog

DCE Raslogs are cleared
SYSTEM Raslogs are cleared
```

To clear all DCE messages on the local switch:

```
switch# clear logging raslog message-type DCE

DCE Raslogs are cleared
```

To clear all SYSTEM messages on the local switch:

```
switch# clear logging raslog message-type SYSTEM

SYSTEM Raslogs are cleared
```

Related Commands

logging raslog console, show logging raslog, show running-config logging

clear mac-address-table conversational

Clears the conversational MAC interface status and configuration information.

Syntax

clear mac-address-table conversational [**address** *mac_address* | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port* | **linecard** *linecard_number* [**rbridge-id** *rbridge-id*] | **vlan** *vlan_id*]

Parameters

address *mac_address*
Specifies a MAC address in HHHH.HHHH.HHHH format.

interface
Specifies an interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

linecard *linecard_number*
Specifies a line card on the local RBridge.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

vlan *vlan_id*
Specifies a VLAN interface.

Modes

Privileged EXEC mode

History

Release version	Command history
5.0.0	This command was introduced.

clear mac-address-table dynamic

Clears the dynamic MAC interface status and configuration information.

Syntax

clear mac-address-table dynamic [**address** *mac_address* | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port* | **vlan** *vlan_id*]

Parameters

address *mac_address*
Specifies a MAC address in HHHH.HHHH.HHHH format.

interface
Specifies an interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

vlan *vlan_id*
Specifies a VLAN interface.

Modes

Privileged EXEC mode

History

Release version	Command history
5.0.0	This command description was modified to distinguish it from the form with the **conversational** keyword, and new keywords were added.

clear nas statistics

Clears automatic network attached storage (NAS) statistics.

Syntax

clear nas statistics all | **server-ip** *ip_addr/prefix* [**vlan** *vlan_id* | **vrf** *VRF_name*] [**rbridge-id** *rbridge-id*]

Parameters

all
Shows all gathered statistics.

server-ip
IP address for which to clear Auto-NAS statistics.

ip_addr/prefix
IPv4 address/prefix of a specified **Auto-** NAS port.

vlan *vlan_id*
Specifies a VLAN interface for which to clear the statistics.

vrf *VRF_name*
Specifies an OSPF VRF interface for which to clear the statistics.

rbridge-id *rbridge-id*
Specifies an RBridge ID for which to clear the statistics.

Modes

Privileged EXEC mode

Examples

```
switch# clear nas statistics all server-ip 1.1.1.0/24
```

clear overlay-gateway

Clear counters for the specified gateway.

Syntax

clear overlay-gateway *name* { **statistics** | **vlan statistics** }

Parameters

name
Specifies the name of the VXLAN gateway profile.

statistics
Clears all statistics for the VXLAN gateway.

vlan statistics
Clears per-VLAN statistics for the VXLAN gateway.

Modes

Privileged EXEC mode

Usage Guidelines

This command is available only for a switch that is in logical chassis cluster mode.

If you specify the VXLAN gateway name, the gateway must already be configured.

If you specify VLAN IDs, these VLANS must already be configured as exported VLANs for the gateway.

Examples

To clear all counters for the already configured VXLAN gateway named gateway1:

```
switch# clear overlay-gateway gateway1 statistics
```

clear policy-map-counters

Provides a mechanism for clearing the policy map counters.

Syntax

clear policy-map-counters [**interface** *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*]

Parameters

interface

Specifies an interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

Modes

Privileged EXEC mode

clear sessions

Logs out the user sessions connected to the switch.

Syntax

clear sessions [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command is not distributed across the cluster. The RBridge ID of the node should be used to log out users connected to the individual nodes.

The **rbridge-id** operand is supported in VCS mode only.

Examples

```
switch# clear sessions rbridge-id 3
This operation will logout all the user sessions. Do you want to continue (yes/no)?: y
```

clear sflow statistics

Clears sFlow statistics from all ports or from a specified port..

Syntax

clear sflow statistics interface [*<N>***gigabitethernet** *rbridge-id/slot/port* | **tunnel**]

Parameters

interface
Specifies an interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

tunnel
Specifies the tunnel interface.

Modes

Privileged EXEC mode

Examples

To clear sFlow statistics:

```
switch# clear sflow statistics
```

clear spanning-tree counter

Clears all spanning-tree counters on the interface.

Syntax

clear spanning-tree counter [**interface** | **port-channel** *number* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

interface

Specifies an interface.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels ranges from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace \ *N***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree counters are cleared for all interfaces.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Examples

To clear spanning-tree counters for all interfaces:

```
switch# clear spanning-tree counter
```

To clear spanning-tree counters for a 10-gigabit Ethernet interface:

```
switch# clear spanning-tree counter interface tengigabitethernet 0/1
```

To clear spanning-tree counters for port-channel 23:

```
switch# clear spanning-tree counter interface port-channel 23
```

Related Commands

show spanning-tree

clear spanning-tree detected-protocols

Clears all spanning-tree detected protocols on the interface.

Syntax

clear spanning-tree detected-protocols [**interface** | **port-channel** *number* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

interface

Specifies an interface.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels ranges from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *N***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree detected protocols are cleared for all interfaces.

Examples

To clear detected protocols for all interfaces:

```
switch# clear spanning-tree detected-protocols
```

To clear detected protocols for a 10-gigabit Ethernet interface:

```
switch# clear spanning-tree detected-protocols interface tengigabitethernet 0/1
```

To clear detected protocols for port-channel 23:

```
switch# clear spanning-tree detected-protocols interface port-channel 23
```

Related Commands

show spanning-tree

clear support

Removes support data such as core files and RAS FFDC files from the switch.

Syntax

clear support [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

This command is executed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

The **rbridge-id** operand is supported in VCS mode only.

Examples

To remove core files from the local switch:

```
switch# clear support
```

clear udld statistics

Clears UDLD statistics.

Syntax

clear udld statistics [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* }]

Parameters

interface

Specifies an interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Clears either all unidirectional link detection (UDLD) protocol statistics or clears the statistics on a specified port.

Examples

To clear UDLD statistics on a specific tengigabitethernet interface:

```
switch# clear udld statistics interface te 5/0/1
```

Related Commands

protocol udld, show udld, udld enable

clear vrrp statistics

Clears VRRP statistics.

Syntax

clear vrrp statistics

clear vrrp statistics [**interface** { *<N>***gigabitethernet** [*rbridge-id*]*/ slot/ port* } | **ve** *vlan_id*]

clear vrrp statistics [**session** *VRID*]

Parameters

interface

Specifies an interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an optional RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies the VE VLAN number.

session *VRID*

Specifies the virtual group ID on which to clear statistics. Valid values range from 1 through 128.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group.

This command is for VRRP and VRRP-E. VRRP-E supports only the **ve***vlan_id* type.

To clear all statistics, use the **clear vrrp statistics** command with no operands.

Examples

To clear all VRRP statistics for all virtual groups:

```
switch# clear vrrp statistics
```

To clear statistics for a 10-gigabit Ethernet interface that has an rbridge-id/slot/port of 121/0/50:

```
switch# clear vrrp stastistics interface tengigabitethernet 121/0/50
```

To clear statistics for a session for a VRRP virtual group called "vrrp-group-25":

```
switch# clear vrrp session 25
```

client-to-client-reflection

Enables routes from one client to be reflected to other clients by the host device on which it is configured.

Syntax

client-to-client-reflection

no client-to-client-reflection

Command Default

This feature is enabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

The host device on which it is configured becomes the route-reflector server.

Use the **no** form of this command to restore the default.

Examples

To configure client-to-client reflection on the host device:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# client-to-client-reflection
```

To disable client-to-client reflection on the host device:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no client-to-client-reflection
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

clock set

Sets the local clock date and time.

Syntax

clock set *CCYY-MM-DDTHH:MM:SS* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

CCYY-MM-DDTHH:MM:SS

Specifies the local clock date and time in year, month, day, hours, minutes, and seconds. Valid date and time settings range from January 1, 1970 to January 19, 2038.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

An active NTP server, if configured, automatically updates and overrides the local clock time. The RBridge ID of the node should be used to set the clock.

The rbridge-id parameter is supported in Logical chassis cluster mode only.

Examples

To set the date and time to March 17, 2010, 15 minutes past noon in Logical chassis cluster mode for all switches in the cluster:

```
switch# clock set rbridge-id all 2010-03-17T12:15:00
```

Related Commands

clock timezone (Privileged EXEC mode), ntp server, show clock

clock timezone (Privileged EXEC mode)

Sets the time zone based on region and longitudinal city.

Syntax

clock timezone *region/city* [**rbridge-id** { *rbridge-id* | **all** }]

no clock timezone [**rbridge-id** *rbridge-id*]

Parameters

region
Specifies the region's time zone.

city
Specifies the city's time zone.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Sets the local clock time zone.

Regions include the following countries: Africa, America, Pacific, Europe, Antarctica, Asia, Australia, Atlantic, Indian, and longitudinal city. For a complete listing of supported regions and cities, refer to time zone appendix in the *Network OS Administrator's Guide* .

By default, all switches are in the Greenwich Mean Time (GMT) time zone. The **no** operand removes the time zone setting for the local clock. When using the **no** operand, you do not need to reference a time zone setting.

The **no** operand is not distributed across the cluster. The RBridge ID of the node should be used.

Network Time Protocol (NTP) commands must be configured on each individual switch.

The region name and city name must be separated by a slash (/).

After upgrading your switch to a new Network OS version, you might need to reset the time zone information.

This command can also be run in RBridge ID configuration mode.

Examples

To set the time zone to Pacific Standard Time in North America on all nodes in the cluster:

```
switch# clock timezone America/Los_Angeles rbridge-id all
```

To remove the time zone setting:

```
switch# no clock timezone rbridge-id 5
```

Related Commands

clock set, ntp server, show clock

clock timezone (RBridge ID configuration mode)

Sets the time zone based on region and longitudinal city.

Syntax

clock timezone *region/city*

no clock timezone

Parameters

region
Specifies the region's time zone.

city
Specifies the city's time zone.

Modes

RBridge ID configuration mode

Usage Guidelines

Sets the local clock time zone.

Regions include the following countries: Africa, America, Pacific, Europe, Antarctica, Asia, Australia, Atlantic, Indian, and longitudinal city. For a complete listing of supported regions and cities, refer to Appendix C in the *Network OS Administrator's Guide* .

By default, all switches are in the Greenwich Mean Time (GMT) time zone. The **no** operand removes the timezone setting for the local clock. When using the **no** operand, you do not need to reference a timezone setting.

The **no** operand is not distributed across the cluster.

Network Time Protocol (NTP) commands must be configured on each individual switch.

The region name and city name must be separated by a slash (/).

Upgrade considerations: Existing timezone of system is retained after firmware upgrade, and it will be updated in configuration settings.

Downgrade considerations: Existing timezone of system will be retained after firmware downgrade and the respective entry will be removed from configuration settings.

This command can also be run in Privileged EXEC configuration mode.

Examples

To set the time zone to Pacific Standard Time in North America on all nodes in the cluster:

```
switch# configure
switch(config)# rbridge-10
switch(config-rbridge-id-10# clock timezone America/Los_Angeles
```

To remove the timezone setting:

```
switch# configure
switch(config)# rbridge-10
switch(config-rbridge-id-10# no clock timezone
```

cluster-id

Configures a cluster ID for the route reflector.

Syntax

cluster-id [*num* | **ipv4-address** *ip-addr*]

no cluster-id

Command Default

The default cluster ID is the device ID.

Parameters

num

Integer value for cluster ID. Range is from 1 through 65535.

ip-addr

IPv4 address in dotted-decimal notation.

Modes

BGP configuration mode

Usage Guidelines

When configuring multiple route reflectors in a cluster, use the same cluster ID to avoid loops within the cluster.

Use the **no** form of this command to restore the default.

Examples

To configure a cluster ID for the route reflector:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# cluster-id 1234
```

compare-med-empty-aspath

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation.

Syntax

compare-med-empty-aspath

no compare-med-empty-aspath

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To configure the device to compare MEDs:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# compare-med-empty-aspath
```

compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Syntax

compare-routerid

no compare-routerid

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To configure the device always to compare device IDs:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# compare-routerid
```

confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier *autonomous-system number*

no confederation identifier *autonomous-system number*

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system (AS) number. The configurable range of values is from 1 to 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the no form of this command to remove a BGP confederation identifier.

Use this command to configure a single AS number to identify a group of smaller ASs as a single confederation.

Examples

To specify that confederation 65220 belongs to autonomous system 100.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# local-as 65220
device(config-bgp-router)# confederation identifier 100
```

History

Release version	Command history
5.0.0	This command was introduced.

confederation peers

Configures subautonomous systems (sub-ASs) to belong to a single confederation.

Syntax

confederation peers *autonomous-system number* [*...autonomous-system number*]

no confederation peers *autonomous-system number* [*...autonomous-system number*]

Command Default

No BGP peers are configured to be members of a BGP confederation.

Parameters

autonomous-system number

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 to 4294967295.

Modes

BGP configuration mode.

Usage Guidelines

Use the no form of this command to remove an autonomous system from the confederation.

Examples

To configure autonomous systems 65520, 65521, and 65522 to belong to a single confederation under the identifier 100.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# local-as 65020
device(config-bgp-router)# confederation identifier 100
device(config-bgp-router)# confederation peers 65520 65521 65522
```

History

Release version	Command history
5.0.0	This command was introduced.

configure terminal

Enters global configuration mode.

Syntax

configure terminal

Modes

Privileged EXEC mode

Related Commands

exit

conform-set-dscp

Configures the packet DSCP priority of a class-map.

Syntax

conform-set-dscp *dscp-num*

no conform-set-dscp *dscp-num*

Parameters

dscp-num

Specifies that traffic with bandwidth requirements within the rate configured for CIR that has the packet DSCP priority set to the value specified by the dscp-num variable. Valid values are 0 through 63.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# conform-set-dscp 3
```

conform-set-prec

Configures the packet IP precedence value of a class-map.

Syntax

conform-set-prec *prec-num*

Parameters

prec-num

Specifies that traffic with bandwidth requirements within the rate configured for CIR will have packet IP precedence value (first 3 bits of DSCP) set to the value in the prec-num variable. Valid values are 0 through 7.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default

switch (config-policymap-class)# police cir 40000

switch(config-policymap-class-police)# conform-set-prec 3
```

conform-set-tc

Configures the CIR internal queue assignment of a class-map.

Syntax

conform-set-tc *trafficclass*

no conform-set-tc *trafficclass*

Parameters

trafficclass

Specifies that traffic with bandwidth requirements within the rate configured for CIR will have traffic class (internal queue assignment) set to the value in the trafficclass variable. Valid values are 0 through 7.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default

switch (config-policymap-class)# police cir 40000

switch(config-policymap-class-police)# conform-set-tc 3
```

connector-group

Designates which connector group that FlexPort is allowed to access on the switch.

Syntax

connector-group *rbridge-id/slot/group*

Command Default

The default connector group is undefined.

Parameters

rbridge-id/slot/port

Specifies a valid Fibre Channel port interface

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

group

Specifies a connector group on the switch. The connector-group numbers range from 1 through 8.

Modes

Hardware configuration mode

Usage Guidelines

This command is supported only on the Brocade VDX 6740 and VDX 2740.

The connector-group numbers are related directly to the ports as numbered on each platform. The connector-group numbers that are allowed to be changed and their associated port numbers are shown in the table below. For example, on a Brocade VDX 6740, ports 1 through 8 belong to connector group 1. Not every connector group is supported on a switch.

TABLE 5 Flexport supported hardware

Platform	Port number range	Connector group
Brocade VDX 6740	1-8	1
	17-24	3
	33-40	5
	41-48	6
Brocade VDX 2740T	43.50	1
	51-56 (6 ports only)	2

Examples

This example sets the connector group for Rbridge-ID 1 to group 1.

```
switch# configure terminal
switch(config)# hardware
switch(config-hw)# connector-group 1/0/1
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

flexport, hardware, speed (FlexPort)

connector

Executes connector mode for the purpose of configuring breakout mode on Quad SFPs (QSFPs).

Syntax

connector [**rbridge-id** *rbridge-id*] *slot/port*

no connector [**rbridge-id** *rbridge-id*] *slot/port*

Parameters

rbridge-id *rbridge-id*

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Hardware configuration mode

Examples

```
switch(config-hardware)# connector 2/0/1
switch(config-connector-2/0/1)#
```

Related Commands

sfp breakout, power-off linecard, power-on linecard, show running-config hardware connector

continue

Configures a route-map instance number that goes in a continue statement in a route-map instance.

Syntax

continue *number*

no continue *number*

Parameters

number

Route-map instance number. Range is from 1 through 4294967295.

Modes

Route map configuration mode

Related Commands

route-map

copy

Copies configuration data.

Syntax

copy *source_file destination_file*

Parameters

source_file

The source file to be copied. Specify one of the following parameters:

default-config

The default configuration.

global-running-config

Global data of the running configuration. (Available in both fabric cluster mode and logical chassis cluster mode.)

local-running-configuration

Local data of the running configuration. (Available in fabric cluster mode only.)

rbridge-running-configuration *rbridge-id*

Running configuration of a specified RBridge. (Available in logical chassis cluster mode only.)

running-config

The running configuration.

startup-config

The startup configuration.

flash://*filename*

A file in the local flash memory.

NOTE

This option is not supported on the Brocade VDX 2740 or Brocade VDX 2746.

ftp://*username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is FTP.

scp://*username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is SCP.

sftp://*username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is SFTP.

tftp://*username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is TFTP.

usb://*path*

A file on an attached USB device.

destination_file

The destination file. Specify one of the following parameters:

default-config
The default configuration.

global-running-config
Global data of the running configuration. (Available in both fabric cluster mode and logical chassis cluster mode.)

local-running-configuration
Local data of the running configuration. (Available in fabric cluster mode only.)

rbridge-running-configuration *rbridge-id*
Running configuration of a specified RBridge. (Available in logical chassis cluster mode only.)

running-config
The running configuration.

startup-config
The startup configuration.

flash://*filename*
A file in the local flash memory.

ftp://*username:password@host_ip_address//path*
A file on a remote host. Transfer protocol is FTP.

scp://*username:password@host_ip_address//path*
A file on a remote host. Transfer protocol is SCP.

sftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is SFTP.

tftp://*username:password@host_ip_address/path*
A file on a remote host. Transfer protocol is TFTP.

usb://*path*
A file on an attached USB device.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to back up and restore configuration files with various protocols.

This command is supported only on the local switch.

IPv4 and IPv6 addresses are supported.

The special characters of dollar sign "$" and exclamation point "!" can be used as part of the password variable, provided they are paired with the correct escape characters. The "$" must be paired with two backslashes "\\". For example, if your password choice was "$password" on a remote server, you must use "username:\\$password@1.1.1.1" for the **copy** command. The exclamation point must be paired with a single backslash in the **copy** command, such as "username:\!password@1.1.1.1".

Examples

To save the running configuration to a file:

```
switch# copy running-config flash://myconfig
```

To overwrite the startup configuration with a locally saved configuration file:

```
switch# copy flash://myconfig running-config
```

To overwrite the startup configuration with a remotely archived configuration file:

```
switch# copy scp://user:password@10.10.10.10//myconfig startup-config
```

To overwrite the startup configuration with a configuration file saved on an attached USB device:

```
switch# copy usb://myconfig startup-config
```

copy default-config startup-config

Restores the startup configuration to the default configuration.

Syntax

copy default-config startup-config

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command copies the default configuration to the current startup configuration. The copy operation effectively resets the startup configuration to factory defaults. It prompts for confirmation because it overwrites the saved startup configuration.

In VCS Fabric mode, all interfaces remain online. The restored default configuration is applied with the exception of the following parameters:

- Interface management IP address
- Software feature licenses installed on the switch
- VCS mode configuration
- Virtual IP address

As of Network OS v4.1.3, if the below configurations exist they are retained after a **copy default-config startup-config** command is executed:

- config -> hardware -> port-group -> mode
- performance config -> hardware -> connector -> sfp breakout

Examples

To restore the default configuration:

```
switch# copy default-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: Y
```

copy running-config startup-config

Copies the running configuration to the startup configuration.

Syntax

copy running-config startup-config [**display-command**]

Parameters

display-command

Displays the configuration commands during the copy operation

Modes

Privileged EXEC mode

Usage Guidelines

This command effectively saves the configuration changes you made to be applied after the switch reboots.

This command prompts for confirmation because it overwrites the startup configuration with the currently active running configuration. When the switch reboots and comes back up, the modified configuration is used.

This command is supported only on the local switch.

Use this command after you have made changes to the configuration.

The running configuration is nonpersistent across reboots.

Examples

To save configuration changes:

```
switch# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: Y
```

copy snapshot (logical chassis cluster mode)

Uploads and downloads configuration snapshot files to and from an FTP or SCP server.

Syntax

copy snapshot rbridge-id *rbridge-id* **snapshot-id** *snapshot-id* **ftp://***directory_path*

copy snapshot rbridge-id *rbridge-id* **snapshot-id** *snapshot-id* **scp://***directory_path*

copy snapshot ftp:// *directory_path* **rbridge-id** *rbridge-id* **snapshot-id** *snapshot-id*

copy snapshot scp:// *directory_path* **rbridge-id** *rbridge-id* **snapshot-id** *snapshot-id*

Parameters

rbridge-id *rbridge-id*
Specifies the RBridge ID whose configuration snapshot has been captured.

snapshot-id *snapshot-id*
Specifies the name of the snapshot that has been captured.

directory_path
Specifies the FTP or SCP directory path to which you are uploading the snapshot or from which you are downloading the snapshot.

Modes

Privileged EXEC mode

Usage Guidelines

This command applies only to nodes that are members of a logical chassis cluster, not a fabric cluster.

If a snapshot was taken on a node that had been disconnected from the cluster, the cluster will not have the snapshot. Therefore, you can use these commands to upload the snapshot from the disconnected RBridge ID to an ftp or scp server, then download it to an RBridge ID on the cluster.

NOTE
The uploaded snapshot configuration file is stored as a tar file (of the form *rbridgeId-snapshotID*) on the FTP or SCP server.

Examples

To upload a snapshot configuration file called node4configuration to an FTP server:

```
switch# copy snapshot rbridge-id 11 snapshot-id node4configuration ftp://backupdir_path
```

Related Commands

vcs config snapshot (logical chassis cluster mode)

copy support

Copies support data to a remote host or a USB device.

Syntax

copy support { **ftp** | **scp** | **support-param** | **usb** } **user** *user_name* **group** *group_name* **password** *password* **host** *ip_address***linecard** *linecard_string* **directory** *dir* [**sub-directory** *dir*] [**timeout** *multiplier*] [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

ftp | **scp** | **usb**

Specifies the File Transfer Protocol (ftp), the Secure Copy Protocol (scp), or the USB directory.

support-param

Enables specification of an optional subdirectory for uploading copy support files.

user *user_name*

Specifies the user login name for the server.

group *group_name*

Specifies the group login name for the server. As many as four group names, separated by commas, can be specified.

password *password*

Specifies the account password.

host *host_ip*

Specifies the host IP address in IPv4 or IPv6 format.

linecard *linecard_string*

Specifies the line card to upload support data. Lx <x=1-4 on M4 platforms, x=1-8 on M8 platforms>.

directory dir

Specifies a fully qualified path to the directory where the support data will be stored.

subdirectory *dir*

Specifies a fully qualified path to the subdirectory where the support data will be stored. (Refer to the Usage Guidelines.)

timeout *multiplier*

Specifies a timeout multiplier. Valid multipliers are 1 through 5. When a timeout multiplier is specified, the default timeout value for each module is multiplied by the specified timeout value.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

all

Specifies all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

The support data is saved in the following format:

```
switchname-IPaddress-slotnumber-cputype-timestamp.modulename.txt.ss.gz
```

Example: sw0-10.123.10.5-S5cp-201204081630.OS.txt.ss.gz

Pagination is not supported with this command. Use the "more" parameter to display the output one page at a time.

The subdirectory is appended to the copy support main directory, which is stored as a Distributed Configuration Manager (DCM) configuration item. DCM supports the configuration management of multinode cluster applications and clustering for VCS.

Examples

To save support data on an attached USB device:

```
switch# usb on

USB storage enabled
switch# copy support usb directory support
```

To copy support data to a subdirectory:

```
switch# copy support support-param sub-directory M8 timeout 3
```

copy support-interactive

Copies support data interactively.

Syntax

copy support-interactive

Modes

Privileged EXEC mode

Usage Guidelines

This command is functionally equivalent to the **copy support** command.

Answering **Y** to the Brocade VCS Fabric support prompt indicates that your switch is in Brocade VCS Fabric mode. Support data will be copied from all nodes in the fabric.

The interactive command interface prompts you for the following information:

- Server Name or IP Address (IPv4 only)
- Protocol (FTP or SCP)
- User login name
- Password
- Directory
- Rbridge ID
- Module timeout multiplier

Examples

To upload support data interactively:

```
switch# copy support-interactive

Save to USB device [y/n]: n
Server Name or IP Address: 10.30.33.131
Protocol (ftp, scp): ftp
User: admin
Password: ********
Directory: /home/admin/support
Enter 'all' for all nodes or specify the rbridgeId(s) of the node(s)[Default: Local Node]: all
Module timeout multiplier[Range:1 to 5.Default:1]: 2
Rbridge-id 195: Saving support information for chassis:sw0, module:RAS...
(output truncated)
```

cos-mutation

Specifies the mutation-map to be used on the port.

Syntax

cos-mutation *map_name*

Parameters

map_name

The user-defined map-name.

Modes

Policy-map configuration mode

Usage Guidelines

This command is allowed only for the Ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set CoS action configured. In this case, the defined CoS takes priority over the mutation map.

Examples

Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# cos-mutation plsmap
```

Related Commands

class, policy-map

counter reliability

Sets and displays the reliability counter for the Access Gateway N_Port Monitoring feature.

Syntax

counter reliability *value*

Command Default

25 SCNs per 5-minute period.

Parameters

value

A value from 10 through 100 static change notifications (SCNs) per 5-minute period.

Modes

Access Gateway (AG) configuration

Usage Guidelines

Use this command while in Access Gateway (AG) mode for a specific RBridge ID. Entering the counter reliability command without a value displays the current counter setting. You can set a value from 10 through 100 SCNs per 5-minute period.

The command sets and displays the reliability count of online and offline SCNs counted during a 5-minute period before the link between an N_Port on a VDX switch in Access mode and an F_Port on an FC fabric is considered unreliable.

Examples

Set the reliability counter value.

```
sw0(config-rbridge-id-3-ag)# counter reliability 50
```

Displays the current reliability counter value.

```
sw0(config-rbridge-id-3-ag)# counter reliability
```

dampening

Sets dampening parameters for the route in BGP address-family mode.

Syntax

dampening { *half-life reuse suppressmax-suppress-time* | **route-map** *route-map* }

no dampening

Parameters

half-life
Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.

reuse
Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.

suppress
Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.

max-suppress-time
Maximum number of minutes a route can be suppressed by the device. Default is 40.

route-map
Enables selection of dampening values established in a route map by means of the **route-map** command.

route-map
Name of the configured route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use **dampening** without operands to set default values for all dampening parameters.

To use the dampening values established in a route map, configure the route map first, and then enter **route-map** followed by the name of the configured route map.

A full range of dampening values (*half-life*, *reuse*, *suppress*, *max-suppress-time*) can also be set by means of the **set as-path prepend** command.

Use the **no** form of this command to disable dampening.

Examples

To enable default dampening as an address-family function:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# dampening
```

To change the all dampening values as an IPv6 address-family function:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# dampening 20 200 2500 40
```

To apply the dampening half-life established in a route map, configure the route map and then use the `set dampening` command:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# route-map myroutemap permit 1
device(config-route-map-myroutemap/permit/1)# set dampening 20
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map, set as-path, set dampening

database-overflow-interval (OSPF)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

0 seconds. If the router enters OverflowState, you must reboot before the router leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

Modes

OSPF VRF router configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

For more information, refer to RFC 1765.

Enter **no database-overflow-interval** to disable the overflow interval configuration.

Examples

To configure a database-overflow interval of 60 seconds:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# database-overflow-interval 60
```

Related Commands

external-lsdb-limit (OSPF)

database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

10 seconds. If the router enters OverflowState, you must reboot before the router leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

Enter **no database-overflow-interval** to disable the overflow interval configuration.

Examples

To configure a database-overflow interval of 120 seconds:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# database-overflow-interval 120
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

external-lsdb-limit (OSPFv3)

debug access-list-log buffer

Configures ACL buffer characteristics.

Syntax

Configure the ACL buffer:
debug access-list-log buffer { **circular** | **linear** } **packet-count** *count_value*

Clear the ACL buffer:
debug access-list-log buffer clear

Parameters

circular | **linear**
Specifies the buffer type.

packet-count *count_value*
Specifies a value from 64 through 2056.

clear
Clears the buffer contents.

Modes

Privileged EXEC mode

debug dhcp packet buffer clear

Clears buffer content from DHCP packet capture.

Syntax

debug dhcp packet buffer clear [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

VRF name mapped to the VRF ID for which the buffer will be cleared. If this operand is not specified, the buffer for the default VRF ID is cleared.

Modes

Privileged EXEC mode

Usage Guidelines

Clears buffer content created from use of the **debug dhcp packet buffer interface** command to enable DHCP packet capture. If the DHCP packet capture is currently enabled, the buffer may fill again.

Examples

The following example clears the buffer content of DHCP packets for the VRF titled "blue".

```
switch# debug dhcp packet buffer clear blue
```

Related Commands

debug dhcp packet buffer interface

debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

Syntax

debug dhcp packet buffer [**circular** | **linear**] [**packet-count** *64-2056*] [**vrf** *vrf-name*] [**interface** *<N>* **gigabitethernet** *rbridge-id/slot/port*]

Command Default

The buffer wraps around to overwrite earlier captures (circular).

Parameters

circular

Buffer wraps around to overwrite earlier captures.

linear

Buffer stops capture when the packet-count value is reached.

clear

Clears the packet buffer.

all

Captures DHCP packets on all interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command configures the capturing buffer behavior by allowing captures to wrap and overwrite earlier captures or stop capturing when a packet-count limit is reached. The current buffer content is cleared when the configuration changes.

Examples

The following example configures a buffer to capture 510 maximum packets in a circular fashion.

```
switch# debug dhcp packet buffer circular packet-count 510
```

Related Commands

debug dhcp packet buffer interface, debug dhcp packet buffer clear, show debug dhcp packet buffer

debug dhcp packet buffer interface

Enables and disables DHCP packet capture on a specific interface.

Syntax

debug dhcp packet buffer interface [*<N>***gigabitethernet** *rbridge-id/slot/port*] [**rx** | **tx**]

no debug dhcp packet buffer interface [*<N>***gigabitethernet** *rbridge-id/slot/port* [**rx** | **tx**]

debug dhcp packet buffer all

no debug dhcp packet buffer all

Parameters

all

Enables DHCP packet capture on all switch interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

rx | **tx**

Specifies whether to capture transmitted or received packets. If not specified, both are captured.

Modes

Privileged EXEC mode

Usage Guidelines

The **all** operand replaces the *interface* operand.

Use the **no** form of this command to disable DHCP packet capture on a specific switch interface when used with **debug dhcp packet buffer interface** [*interface specifications*]

Use the **no** form of this command to disable the DHCP packet capture on all switch interfaces when used with **debug dhcp packet buffer all** .

You can specify a VLAN or physical port for capturing packets. If an interface is not specified, packets are captured on all interfaces.

Examples

The following command enables DHCP packet capture for transmitting data on forty-gigabit Ethernet interface 1/0/1.

```
switch# debug dhcp packet buffer interface te 1/0/1 tx
```

The following command enables DHCP packet capture for receiving data on10-gigabit Ethernet interface 1/0/1.

```
switch# no debug dhcp packet buffer interface te 1/0/1 rx
```

The following command enables DHCP packet capture on all switch interfaces of switch 0.

```
switch# debug dhcp packet buffer all
```

The following command disables DHCP packet capture on all switch interfaces of switch 0.

```
switch# no debug dhcp packet buffer all
```

Related Commands

debug dhcp packet buffer clear, debug dhcp packet buffer, debug fcoe show swcfg, show debug dhcp packet

debug fcoe show swcfg

Displays information related to FCoE classified VLAN configuration in a VIrtual Fabrics context, as well as other parameters.

Syntax

debug fcoe show swcfg

Modes

Privileged EXEC mode

Examples

The following example shows typical output of this command.

```
switch# debug fcoe show swcfg
sw# vlan ivid       ctag       Dom  fcmap    Pri Intvl Tout
=============================================================
0   1002 0x3ea      0x0        10   0x0efc00 3   8000  0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
0   0    0x0        0x0        10   0x000000 0   0     0
```

debug ip

Enables debugging for the IGMP and ICMP traffic on the switch.

Syntax

debug ip packet [**interface** *interface-type interface-number* [**vlan** *vlan_id*] | **count** { **tx** | **rx** } | **icmp** [**interface** *interface-type interface-number*] | **count** *value* | **tx** | **rx** | **igmp** [**interface** *interface-type interface-number*] | **all** | **group** *multicast-grp-address*]

no debug ip packet

Parameters

packet
Enables IP packet debugging.

interface
Displays the IP traffic for the specified interface only.

interface-type
Network interface type (external Ethernet interface, port-channel, or VLAN).

interface-number
Layer 2 or Layer 3 interface number.

vlan *vlan_id*
Specifies a VLAN.

count *value*
Stops display after display count packets. Valid values range from 1 through 32256.

tx
Counts only transmitted packets.

rx
Counts only received packets.

icmp
Displays the ICMP packets.

igmp
Displays the IGMP packets.

all
Enables all IGMP debugging.

group
Enables IGMP debugging for multicast group.

multicast-grp-address
Multicast group address.

Modes

Privileged EXEC mode

Usage Guidelines

When this feature is enabled, all IGMP or ICMP packets received or transmitted are displayed. Debugging can be enabled globally, per interface, or on a multicast group.Use the **no** form of this command to disable debugging.

debug ip bgp

Displays information related to the processing of BGP4, with a variety of options.

Syntax

debug ip bgp [**cli** | **dampening** | **events** | **general** | **graceful-restart** | **ip-prefix** *ip-addr/mask-len* | **ip-prefix-list** *name* | **keepalives** | **neighbor** | **route-map route-selection** | **traces** | **updates** [**rx** | **tx**]]

no debug ip bgp

Parameters

address-family
Displays information about address-family mode.

cli
Displays information about BGP CLI

dampening
Displays BGP4 dampening.

events
Displays all BGP4 events.

general
Displays BGP4 common events.

graceful-restart
Displays BGP graceful restart events.

ip-prefix
Displays information filtered by IP prefix.

ip-addr
IPv4 address in dotted-decimal notation.

mask-len
IPv4 mask length in CIDR notation.

ip-prefix-list
Displays information filtered by IP prefix list.

name
Name of IP prefix list.

keepalives
Displays BGP4 keepalives.

neighbor
Displays BGP information for specified neighbor router.

packet
Displays information about BGP packets.

route-map
Displays configured route map tags.

route-selection
Displays BGP4 route selection.

traces
Displays BGP traces.

updates
Displays BGP4 updates.

rx
Displays BGP4 received updates.

tx
Displays BGP4 transmitted updates

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

To view all BGP4 events:

```
switch# debug ip bgp events
```

To view all BGP4 Graceful restart events:

```
switch# debug ip bgp graceful-restart
```

debug ip bgp address-family ipv4 unicast

Displays information related to the processing of IPv4 address-family support in BGP4.

Syntax

debug ip bgp address-family ipv4 unicast

no debug ip bgp address-family ipv4 unicast

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

Example of typical command.

```
switch# debug ip bgp address-family ipv4 unicast
```

debug ip bgp neighbor

Displays information related to the processing of BGP4 for a specific neighbor.

Syntax

debug ip bgp neighbor *ip-addr*

no debug ip bgp neighbor *ip-addr*

Parameters

ip-addr

IPv4 address in dotted-decimal notation.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

Typical command structure.

```
switch# debug ip bgp neighbor 10.11.12.13
```

debug ip fabric-virtual-gateway

Enables debugging of the Fabric-Virtual-Gateway protocol.

Syntax

debug ip fabric-virtual-gateway { **all** | **fabric** | **nsm** | **cli** | **garp** | **interface ve** *vlan-id* | **ipv4** | **ipv6** }

no debug ip fabric-virtual-gateway {**all** | **fabric** | **nsm** | **cli** | **garp** | **interface ve** *vlan-id* | **ipv4** | **ipv6** }

Command Default

None

Parameters

all
Debugs all that follows the debug option.

fabric
Debugs fabric related events like fabric up or down.

nsm
Debug NSM related events line interface up or down or add or delete.

cli
Debugs CLI related executions or arguments.

garp
Debugs sent gratuitous ARP.

interface ve *vlan-id*
Debugs session level events specified by VLAN ID.

ipv4
Debugs all IPv4 session events.

ipv6
Debugs all IPv6 session events.

Modes

Privileged EXEC mode

Usage Guidelines

Enter the **no** form of the command to disable debugging for the Fabric-Virtual-Gateway protocol.

Examples

The following example enables debugging for all Fabric-Virtual-Gateway protocols.

```
debug ip fabric-virtual-gateway all
```

The following example enables debugging of the fabric for the Fabric-Virtual-Gateway protocol.

```
debug ip fabric-virtual-gateway fabric
```

The following example enables debugging of interface VE 2000 for the Fabric-Virtual-Gateway protocol.

```
debug ip fabric-virtual-gateway interface ve 2000
```

History

Release version	Command history
5.0.1	This command was introduced.

debug ip igmp

Enables or disables debugging for IGMP information.

Syntax

debug ip igmp { **all** | **group** *A.B.C.D* | **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **vlan** *vlan_id* } }

no debug ip igmp

Parameters

all

Displays all values.

group *A.B.C.D*

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

interface

Specifies the interface to be monitored.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

vlan *vlan_id*

Specifies which VLAN interface to display the snooping configuration related information. Refer to the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

When debugging is enabled all of the IGMP packets received and sent, and IGMP-host related events are displayed.

Use the **no** form of this command to disable debugging.

debug ip ospf

Enables debugging for the IP Open Shortest Path First (OSPF) protocol.

Syntax

debug ip ospf { **adj** | **all-vrfs** | **dev** | **error** | **events** | **flood** | **log-debug-message** | **log-empty-lsa** | **ls-id** *A.B.C.D* | **lsa-generation** | **max-metric** | **neighbor** *A.B.C.D* | **packet** | **retransmission** | **route** *A.B.C.D* | **spf** | **vrf** *name* }

no debug ip ospf

Command Default

IP OPSF debugging is disabled.

Parameters

adj
Adjacency related debugs.

all-vrfs
Information for all VRFs instances in a cluster.

dev
Developer debug options.

error
Displays possible errors encountered during time.

events
Events-related debugs.

flood
Flooding-related debugs.

log-debug-message
Debugs message logging.

log-empty-lsa
Empties LSA logging.

ls-id *A.B.C.D*
Link state ID (LSID) debugging for the link-state ID that you specify.

lsa-generation
LSA generation-related debugging.

max-metric
Stub Router Advertisement.

neighbor *A.B.C.D*
Neighbor debugging for the neighbor that you specify.

packet
Packet debugs.

retransmission
Retransmission events.

route *A.B.C.D*
Route debugs for the router that you specify.

spf
SPF trace.

vrf *name*
Debug information for VRF.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no debug ip ospf** to disable IP OPSF debugging.

Examples

To enable adjacency-related debugs:

```
switch# debug ip ospf adj
```

debug ip pim

Enables debugging for IP Protocol Independent Multicast.

Syntax

debug ip pim { **add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all** }

no debug ip pim all

Command Default

All flags are disabled.

Parameters

add-del-oif
Controls the OIF change flag.

bootstrap
Controls the bootstrap processing flag.

group
Controls the processing for a group flag.

join-prune
Controls the Join/Prune processing flag.

nbr-change
Controls the neighbor changes flag.

packets
Controls the packet processing flag.

parent
Controls the parent change processing flag.

regproc
Controls the register processing flag.

route-change
Controls the route changes flag.

rp
Controls the Rendezvous Point (RP) processing flag.

source
Controls the processing for a source flag.

state
Controls the state processing flag.

all
Controls all of the states.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no debug ip pim all** command to disable debugging.

debug ip rtm

Enables debugging for IP RTM.

Syntax

debug ip rtm { *A.B.C.D* | **all** | **counters** { **clear** | **show** } **dump** | **errors** | **fib-comm** | **nexthop** | **port** | **vrf** }

Command Default

IP RTM debugging is disabled.

Parameters

A.B.C.D
Debugs the route specified by this IP address.

all
Enables all debugs.

counters
Enables debug counters.

clear
Clears debug counters.

show
Shows debug counters.

dump
Shows database dump.

errors
Enables internal error debugs.

fib-comm
Debugs communications between the forwarding information base and the routing table manager.

nexthop
Enables next-hop debugs.

port
Enables port database debugs.

vrf
Enables VRF debugs.

Modes

Privileged EXEC mode

Examples

To debug the route specified by the IP address 192.145.12.1:

```
switch# debug ip rtm 192.145.12.1
```

To show a database dump:

```
switch# debug ip rtm dump

Interface       IP-Address      OK?  Method Status     Protocol VRF
Gi 190/0/1      0xbe2a640c      YES  manual up         up       default-vrf
Ve 128          0xa52a800c      YES  manual admin/down up       default-vrf
Ve 1001         0x0a010101      YES  manual admin/down up       default-vrf
Ve 1001         0x65010101      YES  manual admin/down up       default-vrf
Lo 1            0xa02a0c0c      YES  manual up         up       default-vrf
mgmt 1          0x0a14eabe      YES  manual up         up       default-vrf
IP Static Routing Table - 1 entries:
addr: 0x1021f4b8, top 0x1021f590, count 1, default 0 ffffffff
        Type 2
Route_pool:
pool: 101e3bd0, unit_size: 32, initial_number:128, upper_limit:2000000000
  total_number:128, allocated_number:1, alloc_failure 0
  flag: 0, pool_index:1, avail_data:102207b8
Route Entry Pool:
pool: 101e3c80, unit_size: 432, initial_number:128, upper_limit:2000000000
  total_number:128, allocated_number:1, alloc_failure 0
  flag: 0, pool_index:1, avail_data:10221950
Nexthop Settings
 Update: no, Update-always no, Update-Timer 0 Check-Nexthops no
 Recur: yes, Levels 3, Default-enable no
 vrf-count 0, vrf-resolved yes
 Protocols: < connected>
 Nexthops List
  [7] 0xa14e801 hash 7 paths 1 upd last-update-time 0 -> 0xa14e801 mgmt 1
 Nexthop List End
```

debug ip vrf

Displays information related to VRF.

Syntax

debug ip vrf *ip-addr*

no debug ip vrf

Parameters

ip-addr

IPv4 address in dotted-decimal notation.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

Typical command structure.

```
switch# debug ip vrf
```

debug ipv6 dhcpv6 packet buffer

Enables IPv6 DHCPv6 packet capture on an interface or all interfaces.

Syntax

debug ipv6 dhcpv6 packet buffer { **all** | [**interface** [*<N>* **gigabitethernet** *rbridge-id/slot/port*| **ve** *vlan_id*] [**rx** | **tx**] }

no debug ipv6 dhcpv6 packet buffer { **all** | **interface** [*<N>* **gigabitethernet** *rbridge-id/slot/port*| **ve** *vlan_id*] [**rx** | **tx**] }

Command Default

None

Parameters

all

Specifies all buffer packets.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

rx

Specifies the receive direction.

tx

Specifies the receive direction.

ve*vlan_id*

Specifies a virtual Ethernet interface.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command with the appropriate keywords to disable packet capture.

Examples

To enable ICMPv6 packet capture on all interfaces:

```
switch# debug ipv6 dhcpv6 packet buffer all
```

To disable Neighbor Discovery packet capture on an interface in the transmit direction:

```
switch# no debug ipv6 dhcpv6 packet buffer int te 54/0/22 tx
```

History

Release version	Command history
5.0.1	This command was introduced.

debug ipv6 mld

Displays information related to IPv6 Multicast Listener Discovery (MLD), with a variety of options.

Syntax

debug ipv6 mld { **all** | **errors** } | **group** | **interface** [**vlan***vlan_id*] **l2-port** [*<N>* **gigabitethernet** | **port-channel**] | **packet** [**query** | **report**] | **rx** | **tx** }

no debug ipv6 mld { **all** | **errors** } | **group** | **interface** [**vlan***vlan_id*] **l2-port** [*<N>* **gigabitethernet** | **port-channel**] | **packet** [**query** | **report**] | **rx** | **tx** }

Command Default

None

Parameters

all
Displays all information.

errors
Displays error conditions.

group
Displays information for a match group.

interface
Displays information for a specified interface.

vlan*vlan_id*
Specifies a VLAN. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

l2-port
Displays information for a physical or LAG port.

N **gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port).

port-channel
Specifies a port-channel interface.

packet
Displays information related to MLD packets.

query
Displays information for MLD query packets.

report
Displays information for MLD report packets.

rx

Displays information for incoming MLD packets.

tx

Displays information for outgoing MLD packets.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

To view all IPv6 MLD information:

```
switch# debug ipv6 mld all
```

History

Release version	Command history
5.0.0	This command was introduced.

debug ipv6 nd

Displays information related to IPv6 Neighbor Discovery (ND)

Syntax

debug ipv6 nd

no debug ipv6 nd

Command Default

None

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to disable debugging.

Examples

To display information related to IPv6 ND:

```
switch# debug ipv6 nd
```

History

Release version	Command history
5.0.0	This command was introduced.

debug ipv6 ospf

Enables debugging for the IPv6 Open Shortest Path First (OSPF) protocol.

Syntax

debug ipv6 ospf { **ism** | **ism-events** | **ism-status** | **lsa** | **lsa-flooding** | **lsa-generation** | **lsa-install** | **lsa-inter-area** | **lsa-maxage** | **lsa-refresh** | **nsm** | **nsm-events** | **nsm-status** | **packet** | **packet-dd** | **packet-hello** | **packet-lsa-ack** | **packet-lsa-req** | **packet-lsa-update** | **route** | **route-calc-external** | **route-calc-inter-area** | **route-calc-intra-area** | **route-calc-spf** | **route-calc-transit** | **route-install** | **virtual-link** [**all-vrfs** | **rbridge-id** { *rbridge-id* } | **vrf** *vrfname*] }

debug ipv6 ospf { **match-prefix** { *ipv6-addr* | **all** [**all-vrfs** | **rbridge-id** { *rbridge-id* } | **vrf** *vrfname*] }

no debug ip ospf

Command Default

IPv6 OPSF debugging is disabled.

Parameters

ism
Interface State Machine.

ism-events
Interface State Machine events.

ism-status
Interface State Machine status.

lsa
Link State Advertisements.

lsa-flooding
Link State Advertisements flooding.

lsa-generation
Link State Advertisements generation.

lsa-install
Link State Advertisements install.

lsa-inter-area
Inter-area Link State Advertisements.

lsa-maxage
Link State Advertisements max aging.

lsa-refresh
Link State Advertisements refreshing.

nsm
Neighbor state machine.

nsm-events
Neighbor state machine events.

nsm-status
Neighbor state machine status.

packet
OSPFv3 packets.

packet-dd
OSPFv3 data description packets.

packet-hello
OSPFv3 hello packets.

packet-lsa-ack
OSPFv3 LSA ack packets.

packet-lsa-req
OSPFv3 LSA Request packets.

packet-lsa-update
OSPFv3 LSA Update packets.

route
OSPFv3 routes.

route-calc-external
OSPFv3 external route calculation.

route-calc-inter-area
OSPFv3 inter area route calculation.

route-calc-intra-area
OSPFv3 intra area route calculation.

route-calc-spf
OSPFv3 spf route calculation.

route-calc-transit
OSPFv3 transit route calculation.

route-install
OSPFv3 route install.

virtual-link
OSPFv3 virtual links.

all-vrfs
Information for all VRFs instances in a cluster.

vrf *name*
Debug information for VRF.

rbridge-id *rbridge-id*
The physical, loopback, and SVI interfaces specific to the selected RBridge.

match-prefix
Enables match prefix in debug output.

ipv6-addr **Specifies an IPv6 address in dotted-decimal notation.**

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no debug ip ospf** to disable IP OPSF debugging.

Examples

To enable OSPFv3 graceful restart helper debugs:

```
device# debug ipv6 ospf gr-helper
OSPFv3:  gr-helper debugging is on
```

History

Release version	Command history
5.0.0	This command was introduced.

debug ipv6 packet buffer

Enables IPv6 packet capture on an interface or all interfaces.

Syntax

debug ipv6 packet buffer { **all** | **circular packet-count** *count*| **clear** | **interface** [*<N>* **gigabitethernet** *rbridge-id/slot/port*| **ve** *vlan_id*] [**rx** | **tx**] | **linear packet-count** *count* }

no debug ipv6 packet buffer { **all** | **circular packet-count***count*| **clear** | **interface** [*<N>* **gigabitethernet** *rbridge-id/slot/port*| **ve** *vlan_id*] [**rx** | **tx**] | **linear packet-count***count* }

Command Default

None

Parameters

all

Specifies all buffer packets.

circular packet-count

Specifies the number of packets in a circular buffer. Range is from 64 through 2056.

clear

Clears contents of the buffer.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

rx

Specifies the receive direction.

tx

Specifies the receive direction.

ve*vlan_id*

Specifies a virtual Ethernet interface.

linear packet-count

Specifies the number of packets in a linear buffer. Range is from 64 through 2056.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command with the appropriate keywords to disable packet capture.

Examples

To enable ICMPv6 packet capture on all interfaces:

```
switch# debug ipv6 packet buffer all
```

To disable Neighbor Discovery packet capture on an interface in the transmit direction:

```
switch# no debug ipv6 packet buffer int te 54/0/22 tx
```

History

Release version	Command history
5.0.0	This command was introduced.

debug lacp

Enables or disables debugging for the Link Aggregation Control Protocol (LACP).

Syntax

debug lacp { **all** | **cli** | **event** | **ha** | **pdu** [**rx** { **all** | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port* | **tx** { **all** | **sync** | **timer** | **trace level** *number* }

no debug lacp

Command Default

LACP debugging is disabled.

Parameters

all
Turns on all debugging.

cli
Turns on command line interface debugging.

event
Turns on event debugging.

ha
Echo HA events to the console.

pdu
Echo PDU content to the console.

rx all
Turns on debugging for received LACP packets on all interfaces.

rx interface
Turns on debugging for received LACP packets on the specified interface.

interface
Specifies the interface to be monitored.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

tx all
Turns on debugging for transmitted LACP packets on all interfaces.

tx interface
Turns on debugging for transmitted LACP packets on the specified interface.

sync
Echo synchronization to consoles.

timer
Echo timer expiration to console.

trace level *number*
Specifies the trace level number. Valid values range from 1 through 7.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lacp** to disable LACP debugging.

Examples

To enable debugging of LACP PDUs for transmitted and received packets on all interfaces:

```
switch# debug lacp pdu tx all

switch# debug lacp pdu rx all
switch# show debug lacp
LACP rx debugging is on
LACP tx debugging is on
```

Related Commands

show debug lacp

debug lldp dump

Dumps debugging information for the Link Layer Discovery Protocol (LLDP) to the console.

Syntax

debug lldp dump { **all** | [*<N>* **gigabitethernet** *rbridge-id/slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**] }

Command Default

LLDP debugging is disabled.

Parameters

all

Dumps all information to the console.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

Examples

Typical use of this command.

```
switch# debug lldp dump all
LLDP Interface Debug Information for Fo 2/0/49
Admin Status:  RX_TX
Associated Profile:
Link-level FCoE Priority: 0x08 (Configured: No)
Link-level iSCSI Priority: 0x10 (Configured: No)
Link Properties:
    CEE Incapable
    FCoE LLS not Ready
    FCF-Forward Disabled
Sending TLVs:
    CHASSIS_ID: 0x50eb1a173ff1 (MAC)
    PORT_ID: Fo 2/0/49 (IF Name)
    TTL: Hold (4) x Interval (30)
    SYSTEM_NAME
    IEEE_DCBX
    DCBX_FCOE_APP
    DCBX_FCOE_LOGICAL_LINK
    Configured FCoE App
    Configured FCoE Link
    DCBX_CTRL
<truncated>
```

Related Commands

show debug lldp

debug lldp packet

Enables or disables debugging for the Link Layer Discovery Protocol (LLDP).

Syntax

debug lldp packet { **all** | [*<N>***gigabitethernet** *rbridge-id/slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**] }

no debug lldp packet { **all** | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port* }

Command Default

LLDP debugging is disabled.

Parameters

all

Turns on LLDP packet debugging on all interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lldp packet** to disable LLDP debugging.

Examples

To enable debugging of LLDP for both received and transmitted packets on the 10-gigabit Ethernet interface 0/1:

```
switch# debug lldp packet interface tengigabitethernet 0/1 both

switch# show debug lldp

LLDP debugging status:
Interface te0/1    : Transmit Receive
```

Related Commands

show debug lldp

debug show qos drop-reason

Displays the QoS drop reason for one or all interfaces.

Syntax

debug show qos drop-reason interface { [<*N*>**gigabitethernet** *rbridge-id/slot/port*] [**all**] }

Parameters

all

Displays drop-reason information for all interfaces. This option includes all interfaces in a logical chassis that span multiple Rbridges.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

None

Examples

This example displays information the TenGigabitEthernet Interface 1/0/2:

```
switch# debug show qos drop-reason interface tengigabitethernet 1/0/2
Drop Reason Statistics for Interface Te 1/0/2
=============================================
                        Lookup indicates drop: 0000000000
                           Lookup not enabled: 0000000000
                           pause or pfc frame: 0000000000
           non-TRILL port gets all-rbr MAC DA: 0000000000
         MAC SA is bcast/mcast/chassis address: 0000000000
                   type or len err after SNAP: 0000000000
     non-TRILL frame w/o ctrl MAC DA at TRILL: 0000000000
              TRILL outer DA/SA/VLAN mismatch: 0000000000
          TRILL version/mc flag/header error: 0000000000
                        TRILL hop count error: 0000000000
       TRILL SA matches TRILL address of chip: 0000000000
                              Source filtered: 0000000000
                               pre mature EOF: 0000000000
                              IPv4/IPv6 error: 0000000000
                TTL is less than or equal to 1: 0000000000
            IP DA mcast addr mismatches MAC DA: 0000000000
                     IP SA is mcast address: 0000000000
                                IP PIM error: 0000000000
                       IPv4/PIM checksum error: 0000000000
                   IPv4 IHL is greater than 5: 0000000000
                       IP Routing not enabled: 0000000000
                                    Reserved: 0000000000
                             FCoE header error: 0000000000
                      FCoE VSAN hop count error: 0000000000
                       FCoE routing not enabled: 0000000000
                                    Tail Drop: 0000000000
                Drop due to local MAC bit set: 0000000000
                                    Reserved: 0000000000
                               TRILL RPF drops: 0000000000
                                    Reserved: 0000000000
                                 Parity error: 0000000000
                              IPv6 max len error: 0000000000
                           Forward enable error: 0000000000
                                  Policer drops: 0000000000
                        IPv4/IPv6 RPF check fail: 0000000000
                                     Unknown: 0000000000
                                     Unknown: 0000000000
(output truncated)
```

History

Release version	Command history
5.0.0	This command was introduced.

debug spanning-tree

Enables debugging for the Spanning Tree Protocol (STP).

Syntax

debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | **interface port-channel** *number* | <*N*>**gigabitethernet** *slot/port*]] }

no debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | **interface port-channel** *number* | <*N*>**gigabitethernet** *slot/portport*]] }

Command Default

STP debugging is disabled.

Parameters

all

Turns on spanning tree packet debugging on all interfaces.

bpdu

Turns on Bridge Protocol Data Unit debugging.

rx

Turns on debugging for only received spanning-tree packets.

tx

Turns on debugging for only transmitted spanning-tree packets.

interface

Specifies the interface to be monitored.

port-channel *number*

Specifies the port-channel interface. Valid values range from 1 through 6144.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs.

Enter **no debug spanning-tree** to disable debugging.

Examples

To enable debugging of spanning-tree for both Rx and Tx on the 10-gigabit Ethernet interface 0/1:

```
switch# debug spanning-tree bpdu rx interface tengigabitethernet 0/1

switch# debug spanning-tree bpdu tx interface tengigabitethernet 0/1

switch# show debug spanning-tree

MSTP debugging status:
Spanning-tree rx debugging is off
Te 0/1 rx is on
Spanning-tree tx debugging is off
Te 0/1 tx is on
```

Related Commands

show debug spanning-tree

debug udld packet

Enables debugging for the UniDirectional Link Detection (UDLD) protocol.

Syntax

debug udld packet [**all** | { **interface** [<*N*>**gigabitethernet** *rbridge-id/slot/port*] } { **both** | **rx** | **tx** }

no debug udld packet

Command Default

UDLD debugging is disabled.

Parameters

all

Activates UDLD debugging on all ports on the switch.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

both

Sets debugging for both received and transmitted packets.

rx

Sets debugging for received packets only.

tx

Sets debugging for transmitted packets only.

Modes

Privileged EXEC mode

Usage Guidelines

When debugging is enabled UDLD PDUs are written to the console as they are transmitted and/or received on one or all ports.

Use the **show debug udld** command to view your current debug settings.

Use the **no** form of this command to turn off either all dumping of UDLD PDUs or dumping on a specific port.

Examples

To turn on debugging of transmitted packets on a specific tengigabitethernet interface:

```
switch# debug udld packet interface te 5/0/1 tx
```

Related Commands

show debug udld

debug vrrp

Enables debugging for the Virtual Router Redundancy Protocol (VRRP).

Syntax

debug vrrp all

debug vrrp events

debug vrrp packets { **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* } | **recv** | **sent** }

debug vrrp session *VRID*

no debug vrrp all

no debug vrrp events

no debug vrrp packets { **interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* } | **recv** | **sent** }

no debug vrrp session *VRID*

Parameters

all
Debugs all VRRP events, packets, and sessions.

events
Debugs all VRRP events.

packets interface
Debugs packets for an interface that you specify. Also enables the *recv* and *sent* parameters.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve *vlan_id*
Specifies the VLAN number for a virtual Ethernet (VE) interface.

packets recv
Debugs packets received.

packets sent
Debugs packets sent.

session *VRID*
Specifies the virtual group ID to debug. Valid values range from 1 through 128.

Modes

Privileged EXEC mode

Usage Guidelines

When debugging is enabled, event and packet information for all virtual groups or for a specific interface are captured..

This command is for VRRP and VRRP-E. VRRP-E supports only the VE interface type.

Enter **no debug vrrp all** with to disable all VRRP debugging.

Enter **no debug vrrp** followed by specific events or packet parameters to remove a specific VRRP debugging configuration.

Examples

To set debugging on sent and received packets for a 10-gigabit Ethernet interface that has an *rbridge-id/slot/port* of 121/0/50:

```
switch# debug vrrp packets interface tengigabitethernet 121/0/50
```

To set debugging for a session for a VRRP virtual group called *vrrp-group-25* :

```
switch# debug vrrp session 25
```

Related Commands

show debug vrrp

default-information-originate (BGP)

Configures the device to originate and advertise a default BGP4 or BGP4+ route.

Syntax

default-information-originate

no default-information-originate

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To originate and advertise a default BGP4 route:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# default-information-originate
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

default-information-originate (OSPF)

Controls distribution of default information to an OSPF router.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type-1** | **type-2** }]

no default-information-originate

Command Default

The default values vary depending on the Operands settings.

Parameters

always

Always advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.

metric-type

Specifies how the cost of a neighbor metric is determined. The default is **type-1**. However, this default can be changed with the **metric-type** command.

type-1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

type-2

The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the route table manager (whether static or learned from another protocol) to its neighbors.

Enter **no default-information-originate** to disable this command.

Examples

To always advertise the default route using a metric value of 20:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)#router ospf
device(config-router-ospf-vrf-default-vrf)# default-information-originate always metric 20
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

Related Commands

default-metric (OSPF), metric-type

default-local-preference

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

Syntax

default-local-preference *num*

no default-local-preference *num*

Command Default

The default local preference is 100.

Parameters

num

Local preference value. Range is from 0 through 65535.

Modes

BGP configuration mode

Usage Guidelines

Use this command to change the local preference value.

Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

Use the **no** form of this command to restore the default.

Examples

```
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# default-local-preference 200
```

default-metric (BGP)

Changes the default metric used for redistribution.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 1.

Parameters

value

Metric value. Range is from 0 through 65535.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

When routes are selected, lower metric values are preferred over higher ones. The default, the BGP4 Multi-Exit Discriminator (MED) value, is not assigned. .

Use the **no** form of this command to restore the default.

Examples

To configure the device to compare MEDs:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-metric 100
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

default-metric (OSPF)

Sets the default metric value for the OSPF or OSPFv3 routing protocol.

Syntax

default-metric *metric*

no default-metric

Command Default

The default metric value for the OSPF or OSPFv3 routing protocol is 10.

Parameters

metric

OSPF routing protocol metric value. Valid values range from 1 through 65535.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

This command overwrites any incompatible metrics that may exist when OSPF or OSPFv3 redistributes routes. Therefore, setting the default metric ensures that neighbors will use correct cost and router computation.

Enter **no default-metric** to return to the default setting.

Examples

To set the default metric to 20:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-metric 20
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

Related Commands

default-information-originate (OSPF)

default-passive-interface

Marks all OSPF and OSPFv3 interfaces passive by default.

Syntax

default-passive-interface

no default-passive-interface

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPF and OSPFv3 control packets.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPF interfaces. You can use the **ipv6 ospf active** and **ipv6 ospf passive** commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.Use the **no** form of this command to disable it.

Examples

To mark all OSPF interfaces as passive for a specified RBridge:

```
device# configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-passive-interface
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

delete

Deletes a user-generated file from the flash memory.

Syntax

delete *file*

Parameters

file

The name of the file to be deleted.

Modes

Privileged EXEC mode

Usage Guidelines

The delete oeration is final; there is no mechanism to restore the fileThis command is supported only on the local switch.

System configuration files cannot be deleted. If you try to delete a system configuration file, an appropriate message is displayed.

Examples

To delete a user-generated copy of a configuration file:

```
switch# dir

total 24
drwxr-xr-x   2 root     sys          4096 Feb 13 00:39 .
drwxr-xr-x   3 root     root         4096 Jan  1  1970 ..
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 myconfig
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys           697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root         6800 Feb 13 00:37 startup-config
switch# delete myconfig

% Warning: File will be deleted (from flash:)!
Continue?(y/n): y
```

Related Commands

copy, dir, rename, show file

description (interfaces)

Specify a string that contains the description of a specified interface..

Syntax

description *line*

no description

Parameters

line

Specifies characters describing the interface. The string must be between 1 and 63 ASCII characters in length.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no description** to remove the interface description.

Examples

To set the string describing internal 10-gigabit Ethernet interface 101/0/1:

```
switch(config)# interface tengigabitethernet 101/0/1
switch(conf-if-te-101/0/1)# description converged_101
```

Related Commands

interface, interface ve, name (VLAN interfaces), show vlan brief

description (LLDP)

Specifies a string that contains the LLDP description.

Syntax

description *line*

no description

Parameters

line

Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no description** to remove the LLDP description.

Examples

To set the strings describing LLDP:

```
switch(conf-lldp)# description Brocade-LLDP
```

description (Port Mirroring)

Specifies a string that contains the description of the Port Mirroring session.

Syntax

description *line*

no description

Parameters

line

Specifies string that contains the description of the Port Mirroring session. The string must be between 1 and 64 ASCII characters in length.

Modes

Monitor session configuration mode

Usage Guidelines

The string displayed in the running-config file to describe the Port Mirroring session.

Enter **no description** to remove the port mirroring description.

Examples

To set the string describing monitor session 1:

```
switch(config)# monitor session 1
switch(config-mon-sess-1)# description server group 1 switch-cmsh
```

Related Commands

monitor session

description (VRRP)

Describes a VRRP-E interface.

Syntax

description *description*

no description

Parameters

description

Characters describing the VRRP-E interface. The string must be between 1 and 64 ASCII characters in length.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Enter **no description** to remove the description.

Examples

To describe VRRP-E group 10 interface:

```
switch(config)# rbridge-id 101

switch(config-rbridge-id-101)# int ve 25

switch(config-ve-25)# vrrp-extended-group 10

switch(config-vrrp-extended-group-10)# description vrrpe_group_10
```

Related Commands

vrrp-group, vrrp-extended-group

destination

Designates the destination interface for the snooping data for flow-based SPAN.

Syntax

destination *dest_ifname*

no destination *dest_ifname*

Parameters

dest_ifname

The name of the destination interface.

Modes

Monitor session mode

Usage Guidelines

Use the **no destination** *dest_ifname* command to delete the destination interface.

Related Commands

span session

dhcp auto-deployment enable

Enables DHCP auto-deployment on the switch.

Syntax

dhcp auto-deployment enable

Command Default

Disabled

Modes

Privileged EXEC mode

Usage Guidelines

This command will cause a cold/disruptive reboot and will require that Telnet, secure Telnet, or SSH sessions be restarted.

Scenario 1: When you enable DHCP auto-deployment and the system starts to reboot, the DAD process is triggered after configuration replay is complete.

In the case of dual Management Moddule (MM) chassis, the DAD process waits for the dual MMs to be in sync before starting the requested firmware download. However, if you manually issue **firmwaredownload -sb** during this period (after DAD is triggered and before the MM is in sync), DHCP auto-deployment will fail because the previous firmware download takes precedence. If you manually issue **firmwaredownload -sb** before DAD is triggered, DHCP auto-deployment will fail for the same reason.

Scenario 2: You issue the command to enable DAD (answer "Yes" when prompted), but before the system reboot, there is an HA failover. DAD will be cancelled. You must enable DHCP auto-deployment from the new active switch.

Scenario 3: You issue the command to enable DAD, but after the system reboot is invoked, takeover occurs (the previous standby switch becomes the new active switch), DHCP auto-deployment will proceed.

Scenario 4: You manually issue the **firmwaredownload** command, but before the firmware download is completed, you enable DAD from the CLI and answer "Yes" when prompted to reboot the switch. When the switch boots up, even if the DAD process detects that the firmware download is needed, it will fail during the sanity check because the previous incomplete firmware download takes precedence. DHCP auto-deployment will fail.

Related Commands

show dadstatus

diag burninerrclear

Clears the error logs that are stored in the nonvolatile memory. These error logs are stored during POST and systemVerification failures. Error logs are automatically cleared during system verification.

Syntax

diag burninerrclear

Modes

Privileged EXEC mode

Examples

Typical output for this command.

```
switch# diag burninerrclear

Clearing errLog for slot M2
Clearing errLog for slot S1
Clearing errLog for slot S2
Clearing errLog for slot S3
Clearing errLog for slot L4
```

Related Commands

diag clearerror, show diag burninerrshow, show diag burninstatus

diag clearerror

Clears the diagnostic errors encountered during offline diagnostic tests.

Syntax

diag clearerror

Modes

Privileged EXEC mode

Usage Guidelines

This command is valid only on fixed-configuration switches.

Examples

To clear the diagnostic failure status:

```
switch# diag clearerror
```

Related Commands

diag burninerrclear, show diag burninerrshow, show diag burninstatus

diag portledtest

Runs various action modes on the port LED tests and validates the functionality on a given slot-based switch or fixed-configuration switch.

Syntax

diag portledtest [**action** *pattern*] [**ethernet** *rbridgeid/slot/port*] [**fibrechannel** *rbridgeid/slot/port*] [**npass** *count*] [**slot** *slot_id*]

Command Default

All the ports are tested in a switch.

The default number of times to perform the test is 1.

The default **action** is cycle_all

Parameters

action *pattern*

Specifies the LED pattern. Action choices are as follows:

blink-amber

Blink Port status LED amber

blink-green

Blink Port status LED green

cycle-all

Cycle all Port LEDs

status-amber

Turn Port status LED amber

status-green

Turn Port status LED green

turn-off

Turn Port status LED off

ethernet

The logical Ethernet interface name, which is mutually exclusive from the Fibre Channel parameter. By default, all ports are tested.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number

fibrechannel

The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet parameter. By default, all ports are tested.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

npass *count*

Specifies the number of times to perform this test. Valid values range from 1 through 10. The default value is 1.

slot *slot_id*

Specifies the slot identifiers for slot-based systems only.

Modes

Privileged EXEC mode (with the chassis disabled in offline mode)

Usage Guidelines

This test can be run on a single port or on all ports in the blade (slot-based switches) or the switch (fixed-configuration switches).

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of cleanup.

The *rbridge-id* is an optional parameter. If the *rbridge-id* is not specified, the test is assigned to the local RBridge ID.

CAUTION

This is a disruptive command. You must disable the switch and chassis before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

Examples

The following commands allow you to run various action modes on the LEDs and validate the functionality.

In slot-based switches:

```
switch# diag portledtest action cycle-all slot L1

% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest...
Turning Port Status LEDs OFF...
Turning Port Status LEDs AMBER...
Turning Port Status LEDs GREEN...
Turning Port Status LEDs BLINK GREEN...
Turning Port Status LEDs BLINK AMBER...
portLedTest on slot L1 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
switch#
```

In fixed-configuration switches:

```
switch# diag portledtest

% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest ...
Testing Ethernet ports..
STATUS LED OFF test
STATUS LED GREEN test
STATUS LED AMBER test
STATUS LED BLINK GREEN test
STATUS LED BLINK AMBER test
Testing FC ports..
STATUS LED OFF test
STATUS LED GREEN test
STATUS LED AMBER test
STATUS LED BLINK GREEN test
STATUS LED BLINK AMBER test
PASSED.
```

Related Commands

diag portloopbacktest, diag post enable, diag turboramtest

diag portloopbacktest

Runs the port loopback test on a given slot-based switch or fixed-configuration switch. You can run this test on a single port or on all ports in the blade (slot-based switches) or switch (fixed-configuration switches). This functional test verifies the ability of each port to transmit and receive frames by setting up the loopback at various levels and speed modes.

Syntax

diag portloopbacktest [**ethernet** *rbridgeid/slot/port*] [**fibrechannel** *rbridgeid/slot/port*] [**lbmode** *loopback_mode*] [**nframes** *count*] [**slot** *slot_id*] [**spdmode** *mode*]

Command Default

Number of frames (**nframes**) is 16.

Loopback mode (**lbmode**) is 2.

Speed mode (**spdmode**) depends on the platform. On a 10 Gbps port, the default speed mode is 10.

Parameters

ethernet

The logical Ethernet interface name, which is mutually exclusive from the Fibre Channel parameter. By default, all ports are tested.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number

fibrechannel

The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet parameter. By default, all ports are tested.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

lbmode *mode*

Specifies the loopback point for the test. Valid values are 1 (external) or 2 (internal). The default is 2.

nframes *count*

Specifies the number of frames to send. Valid values range from 1 through 16. The default is 16.

slot *slot_id*

Specifies the slot identifiers for slot-based systems only.

spdmode *mode*

Specifies the speed mode for the test. This parameter controls the speed at which each port operates during the test. Valid parameters are as follows: 1 Gbps 2 Gbps 4 Gbps 8 Gbps 10 Gbps 16 Gbps 40 Gbps100 Gbps

Modes

Privileged EXEC mode (with the chassis disabled, in offline mode)

Usage Guidelines

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset or a reinitialization sequence as part of cleanup.

The *rbridge-id* is an optional parameter. If the *rbridge-id* is not specified, the test is assigned to the local RBridge ID.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

Examples

In slot-based switches:

```
switch# diag portloopbacktest slot S1

% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
<..cut..>
portLoopbackTest on ports 0-143 PASSED
portLoopbackTest on slot S1 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
```

In fixed-configuration switches:

```
switch# diag portloopbacktest

% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest ..............
PASSED.
```

Related Commands

diag portledtest, diag post enable, diag turboramtest

diag post enable

Enables and disables the power-on self-test (POST).

Syntax

diag post [*rbridge-id*] **enable**

no diag post [*rbridge-id*] **enable**

Command Default

POST is enabled.

Parameters

rbridge-id

Specifies an RBridge ID on which POST is run.

enable

Enables the power-on self-test on the specified switch.

Modes

Global configuration mode

Usage Guidelines

Following the **diag post enable** command, update the startup-config by copying the running-config to the start-up config, which takes effect during reboot or a power cycle.

Enter **no diag post** [*rbridge-id*] **enable** to disable the POST for that RBridge.

Examples

To enable the POST for a RBridge:

```
switch# config

Entering configuration mode terminal
switch(config)# diag post rbridge-id 1 enable

switch(config)# exit

switch# copy running-config startup-config

This operation will modify your startup configuration. Do you want to continue? [y/n]: y

1970/01/01-09:09:49, [DCM-1101], 2086, M2, INFO, VDX8770-4, Copy running-config to startup-config
operation successful on this node.
```

To disable the POST for an RBridge ID:

```
switch(config)# no diag post rbridge-id 1 enable
```

Related Commands

show running-config diag post

diag prbstest

Runs the Pseudo Random Bit Sequence (PRBS) test on a given slot to verify the back end connections between the line card (LC) and switch fabric module (SFM).

This command also verifies the internal blade connections when executed in LC.

Syntax

diag prbstest slot { **L1** | **L2** | **S1** | **S2 ...** } **pattern** { *pattern* }

Command Default

The default PRBS pattern is PRBS7.

Parameters

slot *slot*

Specifies the slot ID, from 1 through 6. This test is applicable for slot-based systems only.

pattern *pattern*

Specifies the PRBS pattern, from 1 through 8. Valid values are **PRBS7** , **PRBS23** , and **PRBS31** . The default is PRBS7, which is the least stressful pattern, whereas PRBS31 is the most stressful pattern.

Modes

Privileged EXEC mode (with the chassis disabled, in offline mode)

Usage Guidelines

This test is not supported on fixed-configuration switches, nor can it be run on a per-port basis

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

Examples

In slot-based switches:

```
switch# diag prbstest slot L6 pattern PRBS7

% Info: This test should be run to completion. Please do not abort while it is executing.
Running prbstest...
Initializing ASICs & Ports...
Performing Link Training from L6 to S1
Performing Link Training from L6 to S2
Performing Link Training from L6 to S3
Performing Link Training from L6 to S4
Performing Link Training from L6 to S5
<..cut..>
slot S6 ASIC 1 Port 15 Tap0: 0x08 Tap1: 0x33 Tap2: 0x20
Performing Link Testing from L6 to S1
Performing Link Testing from L6 to S2
Performing Link Testing from L6 to S3
Performing Link Testing from L6 to S4
Performing Link Testing from L6 to S5
Performing Link Testing from L6 to S6
prbsTest on slot L6 PASSED
```

Related Commands

diag portledtest, diag portloopbacktest, diag turboramtest

diag setcycle

Configures the user-defined parameters required for the system verification test.

Syntax

diag setcycle

Command Default

Referto the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

If, after you enter the **diag setcycle** command, you respond with **yes** , the following settings are the default values:

- *num_of_runs* : 1. Valid values for number of runs are 1 through 25.
- *min_lb_mode* : 2. Valid values for minimum loopback mode are 1 (external) or 2 (internal). If set to 1, all the external user ports must be connected with small form-factor pluggable devices (SFPs) and loopback plugs.
- *pled_passes* : 1. Valid values for the number of portLedTest loops are 1 through 10.
- *tbr_passes* : 1. Valid values for the number of turboRamTest loops are 1 through 10. This parameter is not supported on fixed configuration switches.
- *plb_nframes* :16. Valid values for the number of portLoopbackTests are 4 through 16.

If you respond with **no** , the system prompts you for these values.

Examples

To change the value of num_of_runs parameter to 3:

```
switch# diag setcycle num_of_runs 3

Setting number_of_runs to 3.
Committing changes to configuration
```

In slot-based switches:

```
0 is not a valid number of passes. See sample below.
rontee128# diag setcycle num_of_runs 0

-------------------------------------^
syntax error: "0" is out of range.
switch# diag setcycle
Do you want use default values [Y/N]?    : y

DEFAULT - KEYWORD       : COMMENT
replacing 2 with default 1
 1      - number_of_runs        : number of passes of verify
 2      - min_lb_mode   : Limits -lb_mode of tests
VERIFY - label : Label for run start and stop messages
 1      - tbr_passes    : turboramtest number of passes
replacing 8 with default 16
 16     - plb_nframes   : portloopbacktest number of frames default speed
 1      - pled_passes   : portledtest number of passes
 1      - prbs_p7       : LC Backplane test with pattern PRBS7+
16     - cplb_nframes  : portloopbacktest in Core Blade number of frames
Committing changes to configuration
switch# diag setcycle

Do you want use default values [Y/N]?     : y

DEFAULT - KEYWORD       : COMMENT
 1      - number_of_runs        : number of passes of verify (0=infinite)
 2      - min_lb_mode   : Limits -lb_mode of tests
 0      - sof   : Enable stop testing on first fail
 VERIFY - label : Label for run start and stop messages
 1      - tbr_passes    : turboramtest number of passes
 16     - plb_nframes   : portloopbacktest number of frames default speed
 0      - plb5_nframes  : portloopbacktest (lb_mode 5) number of frames default speed
 0      - plb7_nframes  : portloopbacktest (lb_mode 7) number of frames
 0      - pled_action   : portledtest action for glowing all led's
 1      - pled_passes   : portledtest number of passes
 1      - prbs_p7       : LC Backplane test with pattern PRBS7+
 0      - prbs_p23      : LC Backplane test with pattern PRBS23+
 0      - prbs_p31      : LC Backplane test with pattern PRBS31+
 0      - cprbs_p7      : SFM Backplane test with pattern PRBS7+
 0      - cprbs_p23     : SFM Backplane test with pattern PRBS23+
 0      - cprbs_p31     : SFM Backplane test with pattern PRBS31+
 16     - cplb_nframes  : portloopbacktest in Core Blade number of frames
 0      - cplb7_nframes : portloopbacktest in Core Blades (lb_mode 7) number of frames
```

In fixed-configuration switches:

```
switch# diag setcycle

Do you want use default values [Y/N]? : y

DEFAULT - KEYWORD : COMMENT
replacing 3 with default 1
1 - number_of_runs : number of passes of verify (0=infinite)
2 - min_lb_mode : Limits -lb_mode of tests
1 - tbr_passes : turboramtest number of passes
16 - plb_nframes : portloopbacktest number of frames default speed
Committing changes to configuration
```

Related Commands

show diag setcycle

diag systemverification

Runs a combination of various hardware diagnostic tests based on the parameters set using the diag setcycle command.

Syntax

diag systemverification [**short**] [**stop**]

Command Default

If *short* is not specified, all the burn-in parameters that control the number of frames are run.

Parameters

short

Sets the burn-in parameters that control the number of frames to one for a quick run.

stop

Stops the current systemVerification run.

Modes

Privileged EXEC mode (with the chassis disabled in offline mode)

Usage Guidelines

The primary use for this command is software regression testing, or a quick validation that all hardware is operational.

CAUTION
This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

Error logs are cleared automatically during system verification.

To check the current run status, enter the **show diag burninstatus** command.

All errors are stored in the non-volatile memory. You can check the error status using the **show diag burninerrshow** command.

During abnormal termination or when terminated by using the stop parameter, the system might be in unusable state. Perform a reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

Examples

To run various tests, such as the memory and portloopback tests, with various combinations:

```
switch# diag systemverification

% Info: This test should be run to completion. Please do not abort while it is executing.
systemverification: burnin parameters.
CURRENT - KEYWORD : DEFAULT
1 - number_of_runs : 1
2 - min_lb_mode :    2
1 - tbr_passes :     1
16 - plb_nframes :  16
<..cut..>
```

diag turboramtest

This test performs a series of low-level structural tests to determine the basic health of the PCI or PCIe bus and the memories inside the switch ASIC.

Syntax

diag turboramtest [**passcnt** *count*] [**slot** *slot_id* }

Command Default

The pass count (**passcnt**) is 1.

Parameters

passcnt *count*

Specifies the number of test repetitions. By default, the test runs once. Valid values range from 1 through 10.

slot *slot_id*

Specifies the slot ID. This is mandatory for slot-based systems only.

Modes

Privileged EXEC mode (with the chassis disabled in offline mode).

Usage Guidelines

During abnormal termination, the system might be in unusable state. Perform reload to reboot the chassis or switch to recover.

In slot-based systems, the blade under test undergoes a reset and/or a reinitialization sequence as part of the cleanup process.

CAUTION

This is a disruptive command. You must disable the chassis and switch before running the test. In addition, you must reload or fastboot the switch or chassis after the test has completed running.

Examples

In slot-based switches:

```
switch# diag turboramtest slot S2

% Info: This test should be run to completion. Please do not abort while it is executing.
Running turboramtest...
Initializing ASIC 0 for BIST
Initializing ASIC 1 for BIST
Initializing ASIC 2 for BIST
turboRamTest on ASIC 0 PASSED
turboRamTest on ASIC 1 PASSED
turboRamTest on ASIC 2 PASSED
turboRamTest on slot S2 PASSED
% Info: Resetting the blade. Please wait till it gets initialized...
completed.
```

In fixed-configuration switches:

```
switch# diag turboramtest

% Info: This test should be run to completion. Please do not abort while it is executing.
Running turboramtest ..............
PASSED.
```

dir

Lists the contents of the switch flash memory.

Syntax

dir

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To list the contents of the flash memory:

```
switch# dir

total 24
drwxr-xr-x   2 root     sys          4096 Feb 13 00:39 .
drwxr-xr-x   3 root     root         4096 Jan  1  1970 ..
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 myconfig.vcs
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys           697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root         6800 Feb 13 00:37 startup-config
```

Related Commands

copy, delete, rename, show file

disable (Fabric-Virtual-Gateway)

Disables the Fabric-Virtual-Gateway session on the VE interface.

Syntax

disable

no disable

Command Default

None

Modes

Fabric-Virtual-Gateway on an RBridge VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

The **no** form of the command inherits the interface VE state from the global configuration.

The session can be disabled at the RBridge level even if it is enabled at the global level.

Examples

The following example shows how to disable a session on a VE interface.

```
switch(config)# rbridge-id 55
switch(config-rbridge-id-55)# interface ve 2000
switch(config-rbridge-Ve-2000)# ipv6 fabric-virtual-gateway
switch(config-ipv6-fabric-virtual-gw)# disable
```

History

Release version	Command history
5.0.1	This command was introduced.

distance (BGP)

Changes the default administrative distances for EBGP, IBGP, and local BGP4 and BGP4+.

Syntax

distance *external-distance internal-distance local-distance*

no distance *external-distance internal-distance local-distance*

Parameters

external-distance
EBGP distance. Range is from 1 through 255.

internal-distance
IBGP distance. Range is from 1 through 255.

local-distance
Local BGP4 and BGP4+ distance. Range is from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

Enter values in the order corresponding to the values in Parameters.

To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones.

Use the **no** form of this command to restore the defaults.

Examples

To configure the device to change the administrative distance:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# distance 100 150 200
```

distance (OSPF)

Configures an administrative distance value for OSPF and OSPFv3 routes.

Syntax

distance { **external** | **inter-area** | **intra-area** } *distance*

no distance

Command Default

The administrative distance value for OSPF and OSPFv3 routes is 110.

Parameters

external
Sets the distance for routes learned by redistribution from other routing domains.

inter-area
Sets the distance for all routes from one area to another area.

intra-area
Sets the distance for all routes within an area.

distance
Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPF or OSPFv3 intra-area route is always preferred over an OSPF or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

Enter **no distance** to return to the default setting.

Examples

To set the distance value for all external routes to 125:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance external 125
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

distribute-list route-map

Creates a route-map distribution list.

Syntax

distribute-list route-map *map* **in**

no distribute-list route-map

Parameters

map
Name of a route map.

in
Creates a distribution list for an inbound route map.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

The distribution list can filter Link State Advertisements (LSAs) received from other OSPF routers and OSPFv3 before adding the corresponding routes to the routing table.

Enter **no distribute-list route-map** to remove the distribution list.

Examples

To create a distribution list using a route map named filter1 that has already been configured:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# distribute-list route-map filter1 in
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

distribute-list prefix-list (OSPFv3)

Applies a prefix list to OSPF for IPv6 routing updates. Only routes permitted by the prefix-list can go into the routing table

Syntax

distribute-list prefix-list *list-name* **in**

no distribute-list prefix-list

Command Default

Prefix lists are not applied to OSPFv3 for IPv6 routing updates.

Parameters

list-name

Name of a prefix-list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates.

in

Applies the prefix list to incoming routing updates on the specified interface.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no distribute-list prefix-list** to remove the prefix list.

Examples

To configure a distribution list that applies the filterOspfRoutes prefix list globally:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# distribute-list prefix-list filterOspfRoutes in
```

History

Release version	Command history
5.0.0	This command was introduced.

dot1x authentication

Enables 802.1Xauthentication on a port.

Syntax

dot1x authentication

no dot1x authentication

Command Default

802.1Xauthentication is disabled for ports.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x authentication** to disable dot1x on the port and remove the configuration from 802.1X management.

Examples

To enable 802.1Xauthentication on a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x authentication
```

To disable 802.1Xauthentication on a specific 40-gigabit Ethernet interface port and remove the configuration from 802.1X management:

```
switch(config)# interface fortygigabitethernet 180/0/6
switch(conf-if-fo-180/0/6)# no dot1x authentication
```

dot1x enable

Enables 802.1X authentication globally.

Syntax

dot1x enable

no dot1x enable

Command Default

Authentication is disabled globally.

Modes

Global configuration mode

Usage Guidelines

Enter **no dot1x enable** to disable 802.1X authentication globally.

Examples

To enable 802.1X authentication globally:

```
switch(config)# dot1x enable
```

dot1x port-control

Controls port-state authorization.

Syntax

dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

no dot1x port-control

Command Default

The default port state is **auto**.

Parameters

auto

Enables authentication on a port. The controlled port is unauthorized until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This has the effect of activating authentication on an 802.1x-enabled interface.

force-authorized

Forces a port to remain in an authorized state. This also allows connection from multiple clients.

force-unauthorized

Forces a port to remain in an unauthorized state.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x port-control** to return to the default setting.

Examples

To enable the port state to auto on a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x port-control auto
```

To enable the port state to force-authorized on a specific 40-gigabit Ethernet interface port:

```
switch(config)# interface fortygigabitethernet 180/0/1
switch(conf-if-fo-180/0/1)# dot1x port-control force-authorized
```

dot1x quiet-period

Sets the number of seconds that a switch remains quiet between a failed authentication and an attempt to retry authentication.

Syntax

dot1x quiet-period *seconds*

no dot1x quiet-period

Command Default

60 seconds

Parameters

seconds

Specifies the time between attempts at authentication. Valid values range from 1 through 65535 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

When a switch cannot authenticate a client, the switch remains idle for the quiet-period interval of time, then attempts the operation again.

Changing the quiet-period interval time to a number lower than the default can result in a faster response time.

Enter **no dot1x quiet-period** to return to the default setting.

Examples

To change the interval time to 200 seconds on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/9)# dot1x quiet-period 200
```

To set the interval time to the default value on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/6
switch(conf-if-fo-180/0/6)# no dot1x quiet-period
```

dot1x reauthenticate interface

Initiates 802.1X reauthentication on a specified interface.

Syntax

dot1x reauthenticate interface [<*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To initiate reauthentication on 10-gigabit Ethernet interface 0/16:

```
switch# dot1x reauthenticate interface tengigabitethernet 0/16
```

dot1x reauthentication

Enables 802.1X port reauthentication.

Syntax

dot1x reauthentication

no dot1x reauthentication

Command Default

Reauthentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x reauthentication** to return to the default setting.

Examples

To enable 802.1X reauthentication on a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x reauthentication
```

To disable 802.1X reauthentication on a specific 1-gigabit Ethernet interface port:

```
switch(config)# interface gigabitethernet 178/2/9
switch(conf-if-gi-178/2/9)# no dot1x reauthentication
```

dot1x reauthMax

Sets the maximum number of times that a port attempts 802.1Xreauthentication before the port changes to the unauthorized state..

Syntax

dot1x reauthMax *number*

no dot1x reauthMax

Command Default

The number of times that a port attempts 802.1X authentication is 2.

Parameters

number

Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. Valid values range from 1 through 10.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x reauthMax** to return to the default setting.

Examples

To set the maximum number of reauthentication attempts to 5 on a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x reauthMax 5
```

To set the reauthentication maximum to the default value on a specific 40-gigabit Ethernet interface port:

```
switch(config)# interface fortygigabitethernet 180/1/9
switch(conf-if-fo-180/1/9)# no dot1x reauthMax
```

dot1x test eapol-capable

Executes the 802.1x readiness check on the switch.

Syntax

dot1x test eapol-capable interface [*<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This comand monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is designated as 802.1x-capable.

If you omit the optional interface keyword, all interfaces on the switch are tested. The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone)The readiness check is not available on a port that is configured with the command **dot1x force-unauthorized** .

Examples

An example of configuring the readiness check:

```
switch# dot1x test eapol-capable interface tengigabitethernet 1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on Ten Gigabit Ethernet1/0/13 is EAPOL capable.
```

dot1x test timeout

Sets the 802.1X readiness test timeout.

Syntax

dot1x test timeout *timeout*

Command Default

10 seconds

Parameters

timeout

Specifies the interval value in seconds. Valid values range from 1 through 65535.

Modes

Global configuration mode

Examples

To set the test timeout to 30 seconds:

```
switch(config)# dot1x test timeout 30
```

Related Commands

dot1x test eapol-capable

dot1x timeout re-authperiod

Sets the number of seconds between reauthorization attempts on a specified interface.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Command Default

3600 seconds

Parameters

seconds

Specifies the seconds between reauthorization attempts. Valid values range from 1 through 4294967295 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x timeout re-authperiod** to return to the default setting.

Examples

To set 25 seconds as the amount of time between reauthorization attempts on a specific 1-gigabit Ethernet interface:

```
switch(config)# interface gigabitethernet 190/0/9
switch(conf-if-gi-190/0/9)# dot1x timeout re-authperiod 25
```

To set the time between reauthorization attempts to the default value on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/5
switch(conf-if-fo-180/0/5)# no dot1x timeout re-authperiod
```

dot1x timeout server-timeout

Sets the 802.1X authentication-sever response timeout for a specified interface.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Command Default

30 seconds

Parameters

seconds

Specifies the number of seconds that a switch waits for the response from the 802.1X authentication server. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no dot1x timeout server-timeout** to return to the default setting.

Examples

To set 40 seconds as the switch-to-authentication server transmission time on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# dot1x timeout server-timeout 40
```

To set the switch-to-authentication server transmission time to the default value on a specific 1-gigabit Ethernet interface:

```
switch(config)# interface gigabitethernet 170/4/2
switch(conf-if-gi-170/4/2)# no dot1x timeout server-timeout
```

Related Commands

dot1x timeout re-authperiod, dot1x timeout supp-timeout, dot1x timeout tx-period, interface

dot1x timeout supp-timeout

Specifies the EAP response timeout for 802.1X authentication.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Command Default

30 seconds

Parameters

seconds

Specifies the number of seconds that the switch waits for a response to the EAP frame. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

This command sets the time in seconds that a switch waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request.

Enter **no dot1x timeout supp-timeout** to return to the default setting.

Examples

To set 45 seconds as the switch-to-client retransmission time for the EAP request frame on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/8
switch(conf-if-te-178/0/8)# dot1x timeout supp-timeout 45
```

To set the switch-to-client retransmission time for the EAP request frame to the default value on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 190/0/16
switch(conf-if-fo-190/0/16)# no dot1x timeout supp-timeout
```

dot1x timeout tx-period

Sets the time the switch waits for a response to an Extensible Authentication Protocol (EAP) request or identity frame.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Command Default

30 seconds

Parameters

seconds

Specifies the time between successive request ID attempts. Valid values range from 1 through 65535 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

This command sets the interval between successive attempts to request an ID (EAP ID Req) or identity frame from the client.

Enter **no dot1x timeout tx-period** to return to the default settings.

Examples

To set 34 as the number of seconds to wait for a response to an EAP-request or identity frame from the client before retransmitting the request on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/16
switch(conf-if-te-190/0/16)# dot1x timeout tx-period 34
```

To set the interval between successive attempts to request an ID (EAP ID Req) to the default value on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 180/0/8
switch(conf-if-fo-180/0/8)# no dot1x timeout tx-period
```

dpod

Manages Dynamic Ports on Demand (POD) assignments.

Syntax

dpod *rbridge-id/slot/port* { **reserve** | **release** }

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a slot number.

port
Specifies a port number.

reserve
Reserves a POD assignment for a port that is currently not able to come online but is expected to be viable in the future. A port license assignment that is reserved will be associated with the first port set that has a vacancy.

release
Removes a port from the port set to which it is currently assigned.

Modes

Global configuration mode

Usage Guidelines

A port POD assignment can only be released if the port is currently offline. Enter **shutdown** to take the port offline.

Do not release a port unless you plan to disconnect the optical link or disable the port persistently. If the link (server or optical) is left in a state where the port could be brought online, the Dynamic POD mechanism will detect this unassigned port and attempt to reassign it to a port set.

This command has no effect on Brocade VDX 8770 switches.

In the Network OS v3.0.0 release this command is supported only on the local switch.

Examples

To reserve a POD assignment:

```
switch(config)# dpod 0/10 reserve

switch(config-dpod-0/10)# exit

switch(config)# dpod 0/11 reserve

switch0(config-dpod-0/11)# exit
```

To remove a port from a POD port set:

```
switch(config)# dpod 5/0/10 release
switch(config-dpod-5/0/10)# exit
switch(config)# dpod 5/0/11 release
switch(config-dpod-5/0/11)# exit
```

Related Commands

show dpod, show running-config dpod

dscp-cos

Specifies a user-defined mutation-map to be used on the port.

Syntax

dscp-cos *map_name*

Parameters

map_name

The user-defined map-name.

Modes

Policy-map configuration mode

Usage Guidelines

This command is allowed only for the Ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set CoS action configured. In this case, defined CoS takes priority over the mutation map.

Examples

Typical command example:

```
switch(config)# policy-map mutation
switch(config-policymap)# class class-default
switch(config-policyclass)# dscp-cos plsmap
```

Related Commands

class, policy-map

dscp-mutation

Specifies the dscp-mutation mutation-map to be used on the port.

Syntax

dscp-mutation *map_name*

Parameters

map_name

The user-defined map-name.

Modes

Policy-map configuration mode-

Usage Guidelines

This command is allowed only for the ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set cos action configured. In this case-defined cos takes priority over the mutation map.

Examples

Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# dscp-mutation plsmap
```

Related Commands

class, policy-map

dscp-traffic-class

Specifies the traffic-class mutation-map to be used on the port.

Syntax

dscp-traffic-class *map_name*

Parameters

map_name

The user-defined map-name.

Modes

Policy-map configuration mode

Usage Guidelines

This command is allowed only for the ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set cos action configured. In this case-defined cos takes priority over the mutation map.

Examples

Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# dscp-traffic-class plsmap
```

Related Commands

class, policy-map

ebs

Configures the excess burst size of a class-map.

Syntax

ebs *ebs-size*

no ebs *ebs-size*

Parameters

ebs-size

Excess burst size. Valid values range from 1250 through 5000000000 bytes in increments of 1 byte.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# ebs 400000
```

edge-loop-detection port-priority

Sets the ELD priority for a port.

Syntax

edge-loop-detection port-priority *eld-priority*

no edge-loop-detection port-priority

Command Default

ELD priority is 128.

Parameters

eld-priority

Specifies the port priority. Valid values range from 0 through 256; a higher number indicates a lower priority.

Modes

Interface subtype configuration mode

Usage Guidelines

The ELD priorityo determines which of the ports involved in a loop will be disabled when the pdu-rx-limit for the Brocade VCS Fabric cluster is reached. The port with the lower priority (higher ELD-priority setting) is the port that is selected to be disabled.

NOTE

If ELD must select between two ports with the same priority, ELD selects the port with the higher port ID to be disabled.

This command applies only in Brocade VCS Fabric mode.

You must use **edge-loop-detection** to enable edge-loop detection separately on the port for the ELD priority to be effective.

Enter **no edge-loop-detection port-priority** to return to the default setting.

Examples

To set the ELD priority of a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 5/0/10
switch(cfg-if-te-5/0/10)# edge-loop-detection port-priority 5
```

To restore the default ELD priority of 128 to a specific 40-gigabit Ethernet interface port:

```
switch(config)# interface fortygigabitethernet 8/1/12
switch(cfg-if-fo-8/1/12)# no edge-loop-detection port-priority
```

edge-loop-detection vlan

Enables edge-loop detection (ELD) on a port and VLAN.

Syntax

edge-loop-detection vlan *vlan-ID*

no edge-loop-detection vlan *vlan-ID*

Command Default

Edge-loop detection is disabled.

Parameters

vlan *vlan-ID*

Specifies a VLAN. (Refer to the Usage Guidelines.)t.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the VLAN parameter to specify a VLAN and port on which to enable edge-loop detection. The port must be a member of the specified VLAN or the command returns an error.

This command applies to Brocade VCS Fabric mode only.

This functionality detects Layer 2 loops only.

Enter **no edge-loop-detectionvlan** *vlan_id* to disable edge-loop detection on the specified VLAN.

Examples

To enable edge-loop detection on VLAN 10 for a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 1/0/7
switch(conf-if-te-1/0/7)# edge-loop-detection vlan 10
```

To disable edge-loop detection on a specific 1-gigabit Ethernet interface port and a VLAN whose ID is 20:

```
switch(config)# interface gigabitethernet 170/1/9
switch(conf-if-gi-170/1/9)# no edge-loop-detection vlan 20
```

eir

Configures the excess information rate for a class-map.

Syntax

eir *eir-rate*

no eir *eir-rate*

Parameters

eir-rate

Excess information rate. Valid values range from 0 through 40000000000 bps in multiples of 40000.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# eir 800000
```

enable

Enables a VRRP-E session.

Syntax

enable

no enable

Modes

Virtual-router-group configuration mode

Usage Guidelines

Use the **no** form of this command to disable a VRRP-E session.

Examples

To enable a VRRP-E sesson on VRRP-E group 10 on interfacxe Ve 25:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-extended-group 10
switch(config-vrrp-extended-group-10)# enable
```

Related Commands

vrrp-extended-group, vrrp-group

enable (Fabric-Virtual-Gateway)

Enables IPv4 or IPv6 Fabric-Virtual-Gateway sessions in VCS.

Syntax

enable

no enable

Command Default

A session under the global VE interface is enabled.

Modes

Fabric-Virtual-Gateway address-family configuration mode

Fabric-Virtual-Gateway under VE interface IPv4 or IPv6 configuration mode

Fabric-Virtual-Gateway on an RBridge VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command to disable a specific IPv4 or IPv6 Fabric-Virtual-Gateway session.

The session can be enabled at the RBridge-level even if it is disabled at global level.

Examples

The following example shows how to enable a Fabric-Virtual-Gateway session in Fabric-Virtual-Gateway address-family configuration mode.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv4
switch(conf-address-family-ipv4)# enable
```

The following example shows how to enable a Fabric-Virtual-Gateway session in Fabric-Virtual-Gateway in VE interface IPv4 configuration mode.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ip fabric-virtual-gateway
switch(config-ip-fabric-virtual-gw)# enable
```

The following example shows how to enable a Fabric-Virtual-Gateway session in Fabric-Virtual-Gateway on an RBridge VE interface IPv6 configuration mode.

```
switch(config)# rbridge-id 55
switch(config-rbridge-id-55)# interface ve 2000
switch(config-rbridge-Ve-2000)# ipv6 fabric-virtual-gateway
switch(config-ipv6-fabric-virtual-gw)# enable
```

History

Release version	Command history
5.0.1	This command was introduced.

enable statistics direction

Enables the collection of per-VLAN statistics for VXLAN overlay gateway tunnels.

Syntax

enable statistics direction { **both** | **tx** | **rx** } **vlan** [**add** | **remove**] *vlan_id*

no enable statistics

Parameters

both
Specifies the collection of statistics for both the receive and transmit directions.

rx
Specifies the collection of statistics for the receive direction.

tx
Specifies the collection of statistics for the transmit direction.

vlan
Specifies a VLAN or range of VLANs to be added or removed for statistics collection.

add
Enables statistics collection on a VLAN ID or range of VLAN IDs. You can use this option if you have disabled specific VLAN IDs and now want to re-enable them.

remove
Disables statistics collection on a VLAN ID or range of VLAN IDs.

vlan_id
A VLAN ID or range of VLAN IDs. The range is from 1 through 4090. See the Usage Guidelines.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

This configuration enables per-VLAN statistics collection for the packets sent and received over the tunnels associated with this gateway instance.

The specified VLAN IDs must already be configured.

If you remove all VLAN IDs from statistics collection, statistics collection becomes disabled and the **remove** option does not appear in the command line interface of the running configuration.

The only way to change the direction once you have executed this command is to enter the **no enable statistics** command, then re-enter the **enable statistics direction** command

The **no** form of this command disables per-VLAN statistics collection for this gateway.

You cannot delete an attached VLAN if statistics collection is enabled on that VLAN.

Examples

To enable statistics collection for all VXLAN tunnels in both directions for VLAN IDs 10and 20 through 30:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# enable statistics direction both vlan 10, 20-30
```

Related Commands

overlay-gateway

end

Returns to the Privileged EXEC command mode from all configuration modes.

Syntax

end

Modes

All configuration modes

Examples

To return to the Privileged EXEC mode from interface configuration mode:

```
switch(config)# interface tengigabitethernet 0/0
switch(conf-if-te-0/0)# end
```

Related Commands

exit, interface

enforce-first-as

Enforces the use of the first autonomous system (AS) path for external BGP (EBGP) routes.

Syntax

enforce-first-as

no enforce-first-as

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

This command causes the router to discard updates received from EGBP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

Use the **no** form of this command to restore the default.

Examples

To configure the device to enforce the use of the first AS path:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# enforce-first-as
```

error-disable-timeout enable

Enables the timer to bring the interface out of the error-disabled state.

Syntax

error-disable-timeout enable

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

When the Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) guard disables a port, the port remains in the disabled state unless the port is enabled manually. This command allows you to enable the interface from the disabled state.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Examples

To bring the interface out of the disabled state:

```
switch(conf-rstp)# error-disable-timeout enable
```

Related Commands

error-disable-timeout interval

error-disable-timeout interval

Sets the timeout for errors on an interface.

Syntax

error-disable-timeout interval *seconds*

no error-disable-timeout interval

Command Default

300 seconds

The timeout feature is disabled.

Parameters

seconds

Specifies the time for the interface to time out. Valid values range from 10 through 1000000 seconds.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Enter **no error-disable-timeout interval** to return to the default setting.

Examples

To set the timeout value to 10 seconds:

```
switch(conf-rstp)# error-disable-timeout interval 10
```

Related Commands

error-disable-timeout enable

exceed-set-dscp

Configures the CIR packet IP precedence of a class-map.

Syntax

exceed-set-dscp *dscp-num*

no exceed-set-dscp *dscp-num*

Parameters

dscp-num

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the dscp-num variable. Valid values are 0 through 7.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default

switch (config-policymap-class)# police cir 40000

switch(config-policymap-class-police)# exceed-set-dscpc 4
```

exceed-set-prec

Configures the CIR packet IP precedence of a class-map.

Syntax

exceed-set-prec *prec-num*

no exceed-set-prec *prec-num*

Parameters

prec-num

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the prec-num variable. Valid values are 0 through 7.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# exceed-set-prec 4
```

exceed-set-tc

Configures the queue assignment of the *trafficclass* variable for a class-map.

Syntax

exceed-set-tc *trafficclass*

no exceed-set-tc *trafficclass*

Parameters

trafficclass

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and is in the limit of what is configured for EIR will have its traffic class (internal queue assignment) set to the value in the trafficclass variable. Valid values are 0 through 7.

Modes

Policy-map class police configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

Example of setting this parameter.

```
switch(config-policymap)# class default

switch (config-policymap-class)# police cir 40000

switch(config-policymap-class-police)# exceed-set-tc 4
```

exit

Exits the current mode and returns to the previous mode.

Syntax

exit

Modes

All command modes

Usage Guidelines

When used in EXEC and Privileged EXEC modes, the **exit** command terminates the session.

Examples

To exit the Interface configuration mode, and return to the global configuration mode:

```
switch(config)# interface tengigabitethernet 0/1

switch(conf-if-te-0/1)# exit

switch(config)# exit
```

Related Commands

enable, interface

extend vlan

Configures switchport VLANs for the tunnels to the containing site in VXLAN overlay gateway configurations.

Syntax

extend vlan { **add** | **remove** } *vlan_id*

no extend vlan

Parameters

add
Specifies a VLAN ID or range of VLAN IDs to be added to a tunnel.

remove
Specifies a VLAN ID or range of VLAN IDs to be removed from a tunnel.

vlan_id
A VLAN ID or range of VLAN IDs. See the Usage Guidelines.

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

The VXLAN Network Identifier (VNI) classification is derived from the "map vlan" configuration of the parent overlay gateway. This command results in the provisioning or unprovisioning of the VLANs. Use the **no extend vlan** *vlan_id* command to unprovision a VLAN.

All of the VLAN IDs that are specified must be VLANs that have been mapped by means of the **map vlan** *vlan_id* **vni** *vni* command on the parent overlay gateway, unless automatic VNI mapping has been enabled by means of the **map vlan vni auto** command.

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing site.

Examples

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing

To configure a switchport VLAN and range of VLANs:

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-overlay-gw-gateway1-site-mysite)# extend vlan add 10,20-30
```

external-lsdb-limit (OSPF)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Command Default

14913080

Parameters

value

Maximum size of the external LSDB. The maximum allowed value is 14913080.

Modes

OSPF VRF router configuration mode

Usage Guidelines

If you change the value, make sure to save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

Enter **no external-lsdb-limit** to return to the default setting.

Examples

To set the limit of the LSDB to 20000:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# external-lsdb-limit 20000
```

Related Commands

database-overflow-interval (OSPF)

external-lsdb-limit (OSPFv3)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Command Default

250000

Parameters

value

Maximum size of the external LSDB. The maximum allowed value is 250000.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

If you change the value, you must save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

Enter **no external-lsdb-limit** to return to the default setting.

Examples

To set the limit of the LSDB to 15000:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# external-lsdb-limit 15000
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

database-overflow-interval (OSPFv3)

Commands F through O

fabric ecmp load-balance

Configures the list of hashing fields.

Syntax

fabric ecmp load-balance [**dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-mac-vid-port** | **src-dst-ip-port** | **src-dst-mac-vid** | **src-mac-vid**]

Parameters

dst-mac-vid
Configures the command to use destination MAC address and VID-based load balancing.

src-dst-ip
Configures the command to use source and destination IP address-based load balancing.

src-dst-ip-mac-vid
Configures the command to use source and destination IP and MAC address and VID-based load balancing.

src-dst-ip-mac-vid-port
Configures the command to use source and destination IP, MAC address, VID and TCP/UDP port-based load balancing.

src-dst-ip-port
Configures the command to use source and destination IP and TCP/UDP port-based load balancing.

src-dst-mac-vid
Configures the command to use source and destination MAC address and VID-based load balancing.

src-mac-vid
Configures the command to use source MAC address and VID-based load balancing.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to configure the list of fields (in the incoming packets), used for hashing.

Examples

To set the ECMP load balance to use source and destination IP address-based load balancing:

```
switch(config)# rbridge-id 2

switch(config-rbridge-id-2)# fabric ecmp load-balance src-dst-ip
```

Related Commands

fabric ecmp load-balance-hash-swap

fabric ecmp load-balance-hash-swap

Configures how to swap the input fields for load balancing.

Syntax

fabric ecmp load-balance-hash-swap *value*

Parameters

value

The control value. Valid values range from 0x0 through 0xFFFFFFFF.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to swap the input fields before feeding them to the hash function.

The variable value for this command is interpreted as the bitwise control of the 212-bit key. Each bit controls whether 2 adjacent bits of the key are to be swapped. This 32-bit control value is written to all four hash swap control registers. This means that this value is replicated in a 32-bit block to form a 106-bit value. A value of 0x0 does not swap any input fields, while a value of 0xffffffff swaps all 106 input bit-pairs.

Related Commands

fabric ecmp load-balance

fabric isl enable

Enables and disables the administration and operational state of an Inter-Switch Link (ISL).

Syntax

fabric isl enable

no fabric isl enable

Command Default

ISL ports are enabled persistently.

Modes

Interface subtype configuration mode

Usage Guidelines

This command functions in Brocade VCS Fabric mode only.

No edge port configuration is allowed on an ISL. If the port is connected to another switch when this command is issued, the fabric may reconfigure.

Enter **no fabric isl enable command** to disable the administration and operational state of an inter-switch link (ISL).

When an RBridge is rejoining the logical chassis cluster, the interface-level configuration is reset to the default values.

Examples

To enable the administration and operational state of an ISL on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 1/0/18
switch(config-if-te-1/0/18)# fabric isl enable
```

To disable the administration and operational state of an ISL on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/1/15
switch(config-if-fo-1/1/15)# no fabric isl enable
```

Related Commands

interface, diag setcycle, show diag burninstatus

fabric neighbor-discovery disable

Disables neighbor discovery for Brocade devices on a per-interface basis.

Syntax

fabric neighbor-discovery disable

no fabric neighbor-discovery

Command Default

Neighbor discovery is enabled by default.

Modes

Interface subtype configuration mode

Usage Guidelines

This command functions in Brocade VCS Fabric mode only.

Use the **no** form of this command to reenable neighbor discovery on this interface.

Examples

To disable neighbor discovery on a specified tengigabitethernet interface:

```
switch# configure
switch(config)# interface tengigabitethernet 1/0/18

switch(config-if-te-1/0/18)# fabric neighbor-discovery disable
```

fabric port-channel

Configures the list of hashing fields for balancing the data load on port-channels.

Syntax

fabric port-channel port_channel_value **load-balance** [**dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-mac-vid-port** | **src-dst-ip-port** | **src-dst-mac-vid** | **src-mac-vid**]

Parameters

port_channel_value
: Configures the command to use destination MAC address and VID-based load balancing.

load-balance
: Configures the command to use destination MAC address and VID-based load balancing.

dst-mac-vid
: Configures the command to use destination MAC address and VID-based load balancing.

src-dst-ip
: Configures the command to use source and destination IP address-based load balancing.

src-dst-ip-mac-vid
: Configures the command to use source and destination IP and MAC address and VID-based load balancing.

src-dst-ip-mac-vid-port
: Configures the command to use source and destination IP, MAC address, VID and TCP/UDP port-based load balancing.

src-dst-ip-port
: Configures the command to use source and destination IP and TCP/UDP port-based load balancing.

src-dst-mac-vid
: Configures the command to use source and destination MAC address and VID-based load balancing.

src-mac-vid
: Configures the command to use source MAC address and VID-based load balancing.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to configure the list of fields (in the incoming packets), used for balancing the load on port-channels.

Examples

To set the port-channel load balance to use both source and destination IP address-based load balancing:

```
switch(config)# rbridge-id 2
 switch(config-rbridge-id-2)# fabric port-channel 10 load-balance src-dst-ip
```

History

Release version	Command history
4.0.0	This command was introduced.

fabric route mcast

Sets the multicast priority for the local RBridge in the fabric.

Syntax

fabric route mcast rbridge-id *rbridge-id* **priority** *priority*

Command Default

Priority is 1.

Parameters

rbridge-id *rbridge-id*

Specifies an RBridge ID.

priority

Sets a priority. The highest priority overrides the lowest RBridge ID and becomes the root.

priority

Specifies the priority number of the RBridge.

Modes

Global configuration mode

Usage Guidelines

The multicast routing information indicates all ports that are members of the multicast distribution tree: ports that are able to send and receive multicast frames. The root of the tree is auto-selected as the switch with the lowest RBridge ID.

Examples

To change an RBridge multicast priority:

```
switch(config)# fabric route mcast rbridge-id 45 priority 5
switch(config)# exit
switch# show running-config fabric route mcast rbridge-id 45 priority
fabric route mcast rbridge-id 45 priority 5
```

Related Commands

show fabric route multicast, show fabric route topology, show running-config fabric route mcast

fabric trunk enable

Enables and disables trunking on a port.

Syntax

fabric trunk enable

no fabric trunk enable

Command Default

Fabric trunking is enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enabling trunking requires an ISL trunking license. You can disable trunking without a license.

This command functions in Brocade VCS Fabric mode only.

ISLs are not allowed on breakout ports.

When the command is executed to update the trunking configuration, the port to which the configuration applies is disabled and subsequently re-enabled with the new trunking configuration. Traffic through the ports may be temporarily disrupted. Enter **no fabric trunk enable** command to disable trunking on a port.

When an RBridge is rejoining the logical chassis cluster, the interface-level configuration is reset to the default values.

NOTE
Trunks are not supported between Brocade 8000 and Brocade VDX 8770 switches.

Examples

To enable a port for trunking on a specific 10-gigabit Ethernet interface port:

```
switch(config)# interface tengigabitethernet 1/0/18
switch(config-if-te-1/0/18)# fabric trunk enable
```

To disable a port for trunking on a specific 40-gigabit Ethernet interface port:

```
switch(config)# interface fortygigabitethernet 8/10/15
switch(config-if-fo-8/10/15)# no fabric trunk enable
```

Related Commands

interface, show fabric trunk

fabric-map

Enables FCoE fabric-map configuration mode. An FCOE fabric-map is equivalent to an FC Virtual-Fabric.

Syntax

fabric-map default

Modes

FCoE configuration mode

Usage Guidelines

The only map name allowed is "default."

You must be in the feature configuration mode for FCoE for this command to function.

Examples

```
switch(config)# fcoe

switch(config-fcoe)# fabric-map default

switch(config-fcoe-fabric-map)#
```

Related Commands

fcoe

fast-external-fallover

Resets the session if a link to an EBGP peer goes down.

Syntax

fast-external-fallover

no fast-external-fallover

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use this command to terminate and reset external BGP sessions of an directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP **timers** command, to expire. This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

Use the **no** form of this command to restore the default.

Examples

To configure the device to reset the session if a link to an EBGP peer goes down:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# fast-external-fallover
```

Related Commands

timers (BGP)

fastboot

Reboots the control processor (CP), bypassing the power-on self-tests (POST).

Syntax

fastboot

Modes

Privileged EXEC mode

Usage Guidelines

This command performs a "cold reboot" (power off and restart) of the control processor, bypassing POST when the system comes back up. Bypassing POST can reduce boot time significantly.

The **fastboot** operation is disruptive, and the command prompts for confirmation before executing. When you reboot a switch connected to a fabric, all traffic to and from that switch stops. All ports on that switch remain inactive until the switch comes back online.

On a modular chassis, the **fastboot** commands only reboots the management module on which the command is executed. If you log in to the switch IP address and execute the fastboot command, only the active management module reboots and POST is bypassed.

Examples

To perform a cold reboot on the switch:

```
switch# fastboot
Are you sure you want to fastboot the switch [y/n]?: y
```

Related Commands

reload

fcmap

Configures the FPMA FCMAP value for an FCoE fabric-map.

Syntax

fcmap *hh:hh:hh*

Command Default

The FPMA FCMAP value is 0E:FC:00.

Parameters

hh:hh:hh

A valid FPMA FCMAP value. Valid values range from 0E:FC:00 through 0E:FC:FF.

Modes

FCoE fabric-map configuration mode

Usage Guidelines

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Examples

```
switch# configuration terminal

switch(config)# fcoe

switch(config-fcoe)# fabric-map default

switch(config-fcoe-fabric-map)# fcmap 0E:FC:00
```

Related Commands

fcoe, fabric-map

fcoe

Enables the FCoE configuration mode.

Syntax

fcoe

Modes

Global configuration mode

Examples

```
switch(config)# fcoe

switch(config-fcoe)#
```

Related Commands

fabric-map

fcoe-enodes

Sets the number of FCoE ENodes that are to be created on a switch.

Syntax

fcoe-enodes *number*

no fcoe-enodes

Command Default

The default value is 64.

Parameters

number

The number of FCoE interfaces. The range is from 0 through 1000.

Modes

RBridge ID configuration mode

FCoE configuration mode

Usage Guidelines

This feature requires an FCoE license. If that license is not present, the number of FCoE ENodes created is 0. When that license is removed, it is recommended that the switch be rebooted. The number of FCoE ENodes created is set to 0 and all interfaces are deleted.

Examples

To set the number of FCoE ENodes to be created to 67:

```
switch(config)# rbridge-id 10
sw0(config-rbridge-id-10)# fcoe
sw0(config-rbridge-fcoe)# fcoe-enodes 67
2013/08/16-09:59:11, [FCOE-1035], 9267, DCE, INFO, sw0, Virtual FCoE port 1/19/65 is online.
2013/08/16-09:59:11, [FCOE-1035], 9268, DCE, INFO, sw0, Virtual FCoE port 1/19/66 is online.
2013/08/16-09:59:11, [FCOE-1035], 9269, DCE, INFO, sw0, Virtual FCoE port 1/19/67 is online.
sw0(config-rbridge-fcoe)#
```

fcoe-profile (AMPP)

Activates the FCoE profile configuration mode for AMPP.

Syntax

fcoe-profile

Modes

Port-profile configuration mode

Usage Guidelines

The only fcoe-profile name allowed is "default".

The FCoE profile configuration mode for AMPP allows configuration of the FCoE attributes of a port-profile.

Examples

```
switch(config)# port-profile default
switch(config-port-profile-default)# fcoe-profile
switch(config-fcoe-profile)# fcoeport default
```

fcoeport

Provisions a port with the default FCoE map.

Syntax

fcoeport *map*

no fcoeport

Parameters

map

This must be **default** .

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to configure a specific port to be an FCoE port with the assigned map name **default**. The only map name allowed is **default**.

Enter **no fcoeport** to remove the FCoE port configuration from the applicable port.

Examples

To provision a specific 10-gigabit Ethernet interface port with the default FCoE map:

```
switch(config)# interface tengigabitethernet 101/0/1

switch(conf-if-te-101/0/1)# fcoeport default
```

Related Commands

interface

fcsp auth

Configures the protocol specific parameters.

Syntax

fcsp auth auth-type dh-chap group { 0 | 1 | 2 | 3 | 4 | * } **hash** { **sha1** | **md5** | **all** } **policy switch** { **on** | **off** | **active** | **passive** }

Parameters

auth-type dh-chap

Authentication type is DH-CHAP.

group

Specifies the DH group value. This parameter sets the strength of the secret. Values are 0, 1, 2, 3, 4 or *. The asterisk (*) indicates all values (0 through 4). The default value is *.

hash

Specifies the hash type used for authentication. Possible values are **sha1**, **md5**, or **all** (sha1 and md5). The default option is **all**.

policy switch

Configures the switch authentication policy attribute. Values are **on**, **off**, **passive**, or **active**. The default switch policy is **passive**.

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

This command configures the authentication policy attributes and controls the policy behavior. The policy configuration includes protocol specific parameters such as authentication type, DH-group value, and hash type. It also defines whether the policy is enabled or disabled and how strictly it is enforced.

The authentication policy can be set to any of these values:

- ON — Strict authentication is enforced on all E-ports. The ISL goes down (port disable) if the connecting switch does not support the authentication or the policy is OFF. During switch initialization, authentication is initiated on all E-ports automatically. The authentication is initiated automatically during the E-port bring-up by fabric module. The authentication handshaking is completed before the switches exchange the fabric parameters (EFP) for E-port bring-up.
- ACTIVE — In this policy, the switch is more tolerant and can be connected to a switch with any type of policy. During switch initialization, authentication is initiated on all E-ports, but the port is not disabled if the connecting switch does not support authentication or the authentication policy is OFF. The authentication is initiated automatically during the E_Port bring-up.
- PASSIVE (default) — The switch does not initiate authentication, but participates in authentication if the connecting switch initiates authentication. The switch does not start authentication on E_Ports, but accepts the incoming

authentication requests, and will not disable if the connecting switch does not support authentication or the policy is OFF.

- OFF — The switch does not support authentication and rejects any authentication negotiation request from neighbor switch. A switch with the policy OFF should not be connected to a switch with policy ON, since the ON policy is strict and disables the port if any switch rejects the authentication. DH-CHAP shared secrets should be configured before switching on the policy from OFF state.

After the authentication negotiation succeeds, the DH-CHAP authentication is initiated. If DH-CHAP authentication fails, the port is disabled. This behavior applies to all modes of the policy.

Authentication policy configuration is not distributed across the cluster. The rbridge-id of the node should be used to configure protocol and policy configurations.

Examples

NOTE
This command is not distributed across the cluster. The RBridge ID of the node should be used to configure protocol and policy configurations.

To set only the authentication type:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# fcsp auth auth-type dh-chap
```

To set only the hash type:

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fcsp authhashsha1
```

To activate the device authentication policy:

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fcsp authpolicy switch active
```

Related Commands

fcsp auth-secret dhchap, show fcsp auth-secret dh-chap, show running-config fcsp auth

fcsp auth-secret dhchap

Sets the shared secret for DH CHAP authentication.

Syntax

fcsp auth-secret dhchap node *switch_wwn* **peer-secret** *secret_key* **local-secret** *secret_key*

no fcsp auth-secret dhchap node *switch_wwn*

Parameters

node *switch_wwn*
Specifies the world wide name (WWN) of the peer.

peer-secret *secret_key*
Specifies the secret of the peer that authenticates the peer to the local switch.

local-secret *secret_key*
Specifies the local secret that authenticates the local switch to the peer.

Modes

Privileged EXEC mode

Usage Guidelines

The local and peer secret keys must be between 8 and 40 characters long.

Only the following non-alphanumeric characters are valid for the secret key:

@ $ % ^ & * ( ) _ + - < > { } [ ] ; ' :

This command is supported on the Brocade VDX 6740 and Brocade VDX 2740.

Enter **no fcsp auth-secret dhchap node***switch_wwnn* to remove the DHCHAP authentication secrets from the data base, so that the switch with the given WWN cannot connect to the local switch.

Examples

To set the shared secret for DH-CHAP authentication:

```
switch# fcsp auth-secret dhchap node 50:00:51:ed:2d:c0:1e:64 \peer-secret 12345678 local-secret 87654321
```

To remove the DH-CHAP authentication secrets from the database:

```
switch# no fcsp auth-secret dh-chap node 50:00:51:ed:2d:c0:1e:64
Shared secret successfully removed
```

Related Commands

fcsp auth, show fcsp auth-secret dh-chap, show running-config fcsp auth

fec-enable

Configures the state of the Forward Error Correction (FEC) on an interface port.

Syntax

fec-enable

no fec-enable

Modes

Interface configuration mode

Usage Guidelines

Use the no form of the command to disable FEC.

Examples

To configure FEC for an interface port.

```
switch(config)# interface fibre-channel 1/0/1
switch(conf-if-fi-1/0/1)# fec-enable
```

History

Release version	Command history
5.0.0	This command was introduced.

fill-word

Configures the link initialization and fill word primitives for an 8-Gbps Fibre Channel port.

Syntax

fill-word { **idle-idle** | **arbff-arbff** | **idle-arbff** | **aa-then-ia** }

Command Default

The **fill-word** value is **idle-idle**.

Parameters

idle-idle

Sets IDLE mode for the link initialization and IDLE as the fill word.

arbff-arbff

Sets ARB(ff) for the link initialization and ARB(ff) as the fill word,

idle-arbff

Sets IDLE mode for the link initialization and ARB(ff) as the fill word,

aa-then-ia

Attempts **arbff-arbff** first. If the attempt fails, goes into **idle-arbff** mode. The **aa-then-ia** mode is preferable as it captures more cases.

Modes

Interface Fibre Channel configuration mode

Usage Guidelines

By default, this command disables and re-enables the port and the port comes online with the new fill word setting.

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6740), in Brocade VCS Fabric mode, and with the FCoE license installed.

This command should be left at the default setting unless the remote port requires a specific setting for fill word.

Examples

To set the fill word Fibre Channel port attribute:

```
switch(config)# interface FibreChannel 7/0/2
switch(config-FibreChannel-7/0/2)# fill-word arbff-arbff
```

filter-change-update-delay

Sets a delay to change the delay in the filter-change status prompt from the default.

Syntax

filter-change-update-delay *delay_time*

no filter-change-update-delay

Command Default

The default value is 10.

Parameters

delay_time

The delay, in seconds, in the filter-change status prompt. Range is from 0 through 600.

Modes

RBridge ID configuration mode

Usage Guidelines

Enter 0 (zero) or use the **no** form of this command to disable the timer.

fips root disable

Permanently disables root access to a switch for compliance with Federal Information Processing Standards (FIPS).

Syntax

fips root disable

Command Default

Root access is enabled.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to disable root access to a switch permanently when preparing the switch for FIPS compliance. Refer to the *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "fibranne" to make the command available.

This command applies only in fabric cluster mode. It can be issued only from a user account with the admin role assigned.

CAUTION
Once root access is disabled, it cannot be re-enabled.

Examples

To disable root access to a switch:

```
switch# unhide fips

Password: *****

switch# fips root disable

This operation disables root account. Do you want to continue? [yes,NO] yes
```

fips selftests

Enables Federal Information Processing Standards (FIPS) self tests which will be performed when the switch boots. If the tests run successfully, the switch comes up in the FIPS compliant state.

Syntax

fips selftests

Command Default

The switch operates in the non-FIPS compliant state.

Modes

Privileged EXEC mode

Usage Guidelines

The FIPS self tests include known answer tests (KATs) that exercise various features of FIPS algorithms and conditional tests that test the randomness of random number generators and check for signed firmware. These tests run when the switch boots. Successful completion of these tests places the switch into the FIPS-compliant state. If any test returns an error, the switch reboots and runs the tests again. Whether tests succeed or fail, you cannot return the switch to the non-FIPS compliant state.

Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "fibranne" to make the command available.

You typically use this command after disabling non-FIPS compliant features on the switch and configuring secure ciphers, but before zeroizing the switch with the **fips zeroize** command. These non-FIPS compliant features that must be disabled include Brocade VCS Fabric mode, the Boot PROM, root access, TACACS+ authentication, and the dot1x feature. Secure ciphers that must be configured are for the SSH protocol and (optionally) for the Lightweight Directory Access Protocol (LDAP) protocol. The **fips zeroize** command erases all critical security parameters and reboots the switch. Refer to *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

This command applies only in fabric cluster mode. It can be entered only from a user account with the admin role assigned.

CAUTION
This command should be used only by qualified personnel. Once a switch is in the FIPS-compliant state, you cannot return it to the non-FIPS compliant state.

Examples

To enable the FIPS self tests:

```
switch# unhide fips

Password: *****

switch# fips selftests

Self tests enabled
```

fips zeroize

Removes all critical security parameters from a switch in readiness for compliance with Federal Information Processing Standards (FIPS) and reboots the switch.

Syntax

fips zeroize

Command Default

The switch operates in the non-FIPS compliant state.

Modes

Privileged EXEC mode

Usage Guidelines

This command erases all critical security parameters from the switch in readiness for FIPS compliance including passwords, shared secrets, and private keys. This command also reboots the switch. If FIPS self tests are enabled and they run successfully during reboot, then the switch comes up in the FIPS-compliant mode. If the FIPS self tests return errors, the switch reboots and runs the tests again.

Under normal operation, this command is hidden to prevent accidental use. Enter the **unhide fips** command with password "fibranne" to make the command available.

Typical use of this command is after disabling non-FIPs compliant features, configuring secure ciphers, and enabling FIPS self tests with the **fips selftests** command. These non-FIPS compliant features that must be disabled include Brocade VCS Fabric mode, the Boot PROM, root access, TACACS+ authentication, and the dot1x feature. Secure ciphers that must be configured are for the SSH protocol and (optionally) for the Lightweight Directory Access Protocol (LDAP) protocol. Refer to the *Network OS Administrator's Guide* for details about preparing a switch for FIPS compliance.

This command applies only in fabric cluster mode. This command can be entered only from a user account with the admin role assigned.

CAUTION
This command should be used only by qualified personnel. Once a switch is in the FIPS-compliant state, you cannot return it to the non-FIPS compliant state.

Examples

To erase all critical security parameters from a switch:

```
switch# unhide fips

Password: *****

switch(config)# fips zeroize

This operation erases all passwords, shared secrets, private keys etc. on the switch. Do you want to
continue? [yes,NO] yes
```

Related Commands

fips selftests, prom-access disable, show prom-access, unhide fips

firmware activate

Activates the firmware in the local or remote nodes after installing the firmware that was downloaded with firmware download noactivate command.

Syntax

firmware activate [**rbridge-id** { *rbridge-id* } | **all** }]

Command Default

Activation of the firmware is performed manually by default after a download.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

noactivate

Downloads the firmware without activating it.

Modes

Privileged EXEC mode

Usage Guidelines

By default, the **firmware download** command downloads the firmware to the system, reboots the system, and commits the firmware automatically. You can specify the **noactivate** parameter to download the firmware to the system without activating it (the node is not rebooted). The user can run the **firmware activate** command later to activate the firmware.

Examples

To activate firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware activate rbridge-id rid1-rid3,rid5
```

firmware commit

Commits a firmware upgrade.

Syntax

firmware commit

Modes

Privileged EXEC mode

Usage Guidelines

The **firmware download** command updates the secondary partitions only. When the **firmware download** command completes successfully and the switch reboots, the system swaps partitions. The primary partition (with the previous firmware) becomes the secondary partition, and the secondary partition (with the new firmware) becomes the primary partition.

By default, **firmware download** automatically commits the firmware after the switch reboots. If you disable auto-commit mode when running **firmware download**, you must execute **firmware commit** to commit the new firmware to the secondary partition.

This command is supported only on the local management modules.

You must run the **firmware download** command with the **nocommit** parameter set for the following firmware commit operation to succeed.

Examples

To commit the firmware:

```
switch# firmware commit

Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
.............
FirmwareCommit completes successfully.
```

Related Commands

firmware download, show versionshow version

firmware download

Downloads the firmware on the local switch.

Syntax

firmware download { **default-config** | **ftp** | **scp** | **sftp** | **usb** | **interactive** } [**manual**] [**nocommit**] [**noreboot**] [**noactivate**] [**coldboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**vcs-mode** *vcsmode*] [**vcs-id** *vcsID*] [**rbridge-id** *rbridge-id*]]

Command Default

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate** to download the firmware to the system without activating it (the node is not rebooted). The user can run **firmware activate** later to activate the firmware.

Parameters

default-config

Sets the configuration back to default except for the following parameters: VCS mode, VCS ID, and RBridge ID. These three parameters are retained except when the options to change their values are specified.

ftp | **scp** | **sftp** | **usb**

Valid protocols are **ftp** (File Transfer Protocol) or **scp** (Secure Copy), **sftp** (SSH File Transfer Protocol), **usb** (universal serial bus). The values are not case-sensitive.

interactive

Runs firmware download in interactive mode. You are prompted for input.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a Top-of-Rack (ToR) switch or in a chassis with only one management module.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually.

noactivate

Downloads the firmware to the system without activating it.

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

host

Specifies the host by DNS name or IP address.

hostname
Specifies an IPv4 DNS host name.

host_ip_address
Specifies the host IP address. IPv4 and IPv6 addresses are supported.

directory *directory*
Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*
Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

user *username*
Specifies the user login name for the host.

password *password*
Specifies the account password.

vcs-mode *vcsmode*
Specifies the new VCS mode. If not set, the existing VCS mode is used. It is only available in local firmware download.

vcs-id *vcsID*
Specifies the new VCS ID. If not set, the existing VCS ID is used. It is only available in local firmware download.

rbridge-id *rbridge-id*
Specifies the new RBridge ID. If not set, the existing RBridge ID is used. It is only available in local firmware download. ,

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partition. This command supports firmware upgrades on the local switch only.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

In a dual-MM system, if you specify the **manual** option with the **default-config** option, make sure you execute the same command on both MMs. After firmware download is completed on both MMs, you must reboot them at the same time. Otherwise, the MMs may run into configuration mismatch issues.

Examples

In logical chassis cluster mode, you have the option to download firmware to multiple nodes:

```
switch# firmware download interactive

Do you want to download to multiple nodes in the cluster? [y/n]: y
Server name or IP address:
```

To perform a manual firmware download to a single management module:

```
switch# firmware download interactive

Server name or IP address: 10.31.2.25

File name: /users/home50/dist/NOSv5.0.0

Protocol (ftp, scp): ftp

User: admin

Password: **********

Do manual download [y/n]: y

Reboot system after download? [y/n]: y

Do Auto-Commit after Reboot? [y/n]: y

System sanity check passed.
You are running a firmware download on dual MM system with 'manual' option. This will upgrade the
firmware only on the local MM.
This command will cause a cold/disruptive reboot and will require that existing telnet, secure telnet
or SSH sessions be restarted.
Do you want to continue? [y/n]: y

(Output truncated)
```

To download firmware to a local node:

```
switch# firmware download protocol ftp host 10.1.2.30 user fvt password pray4green path /dist file
release.plist
This command will download the firmware to the local node. You will need to run firmware activate to
activate the firmware after this command completes.
Do you want to continue? [y/n]: y
2010/01/29-23:48:35, [HAM-1004], 226, switchid 1, CHASSIS | VCS, INFO, Brocade_switch,
Firmwaredownload has started on the switch.
```

To download firmware using the **default-config** option with VCS mode 1, VCS ID 7, and RBridge 10, use the following command:

```
sw0# firmware download default-config ftp host 10.20.1.3 user fvt password pray4green directory dist
file release.plist vcs-mode 1 vcs-id 7 rbridge-id 10
Performing system sanity check...
This command will set the configuration to default and set the following parameters: vcs-mode, vcs-id
and rbridge-id.
This command will cause Cold reboot on both MMs at the same time and will require that existing telnet,
secure telnet or SSH sessions be restarted.
Do you want to continue? [y/n]: y
host 10.20.1.3 user fvt password pray4green directory dist file release.plist
Performing system sanity check...
This command will set the configuration to default and set the following parameters: vcs-mode, vcs-id
and rbridge-id.
This command will cause Cold reboot on both MMs at the same time and will require that existing telnet,
secure telnet or SSH sessions be restarted.
Do you want to continue? [y/n]: y
```

Related Commands

firmware commit, firmware restore, show firmwaredownloadstatus, show versionshow version

firmware download ftp

Specifies FTP as the protocol used to perform a firmware download.

Syntax

firmware download ftp [**coldboot**] [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*]

Command Default

By default, downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivatefirmware download** to download the firmware to the system without activating it (the node is not rebooted). The user can run **firmware activate** later to activate the firmware.

Parameters

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a compact switch or in a chassis with only one management module.

noactivate

Performs a firmware download without activation on the local switch.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.

password *password*
Specifies the account password.

user *username*
Specifies the user login name for the host.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partitionThis command supports firmware upgrades on the local switch only.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

firmware download interactive

Allows the user to select firmware download parameters interactively before starting a firmware download.

Syntax

firmware download interactive

Command Default

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partition.This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

To perform a firmware download in interactive mode using default parameters:

```
switch# firmware download interactive

firmware download interactive
Server name or IP address: 10.31.2.25

File name: /users/home40/Builds/NOS_v5.0.0

Protocol (ftp, scp, sftp): ftp

User: fvt

Password: **********

Do manual download [y/n]: n

System sanity check passed.
Do you want to continue? [y/n]: y
```

firmware download logical-chassis

Downloads the firmware onto the switches.

Syntax

firmware download logical-chassis default-config { **ftp** | **scp** | **sftp** } **host** *host_ip* **user** *username* **password** *password* **path** *path* [**rbridge-id** { *rbridge-id* | **all** }] [**auto-activate**]

Command Default

After firmware is downloaded to the nodes, the command returns without rebooting the nodes. You will need to run **firmware activate** to active the new firmware on the nodes.

Parameters

default-config
Sets the configuration back to default except the following parameters: VCS mode, VCS ID, and RBridge ID. These three parameters are retained.

ftp
Specifies FTP as the protocol used to download the firmware.

scp
Specifies SCP as the protocol used to download the firmware.

sftp
Specifies SFTP as the protocol used to download the firmware.

host *host_ip*
Specifies the host IP address.

user *username*
Specifies the username.

password *password*
Specifies the password.

path *path*
Specifies the filename path where the firmware is located.

auto-activate
Specifies to automatically activate the firmware on the switches after installing the firmware.

coldboot
Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command is controlled by a principal node (coordinator) and executed on individual nodes in the VCS cluster. All sanity check error and warning messages are displayed on the coordinator user session. If an error results during the Installation, the firmware download request is aborted.

Examples

To activate firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware activate rbridge-id rid1-rid3,rid5
```

To perform a firmware recovery on all switch nodes:

```
switch# firmware recover rbridge-id all
```

To automatically activate firmware on switch nodes rbridge-id 161 and 62 when in logical chassis cluster mode:

```
switch# firmware download logical-chassis scp host 10.31.2.25 user release user password releaseuser
directory /pub/sre/SQA/nos/nos5.0.0/nos5.0.0_bld42 auto-activate rbridge-id 161,62
```

To reboot switches in a specific order, which can be done from any node:

```
switch# firmware download logical-chassis rbridge-id all
 path
 path.
firmware activate rbridge-id 2

firmware activate rbridge-id 3
firmware activate rbridge-id 4
firmware activate rbridge-id 1
```

To download firmware using the **default-config** option, use the following command:

```
sw0# firmware download logical-chassis default-config ftp host 10.1.2.30 user fvt password brocade
directory /dist/nos/5.0.0bld26 file release.plist rbridge-id 1,2-3
Rbridge-id       Sanity Result   Current Version
-----------------------------------------------------
   1          Disruptive           5.0.0
   2          Disruptive           5.0.0
   3          Disruptive           5.0.0
You are invoking firmware download with the provision option. This command will download the new
firmware to the specified nodes, default their configuration, and reboot them automatically.
Do you want to continue? [y/n]: y
```

firmware download scp

Specifies SCP as the protocol used to perform a firmware download.

Syntax

firmware download scp [**coldboot**] [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**]

Command Default

A filename is optional. If no filename is specified, release.plist, is used.

Parameters

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

manual

Performs a firmware download on the local switch.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition. (Skips auto-commit after firmware download.)

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

user *username*

Specifies the user login name for the host.

password *password*

Specifies the account password.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional.

noactivate

Performs a firmware download without activation on the local switch.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partitionThis command supports firmware upgrades on the local switch only.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

firmware download sftp

Specifies SFTP as the protocol used to perform a firmware download.

Syntax

firmware download sftp [**coldboot**] **directory** *directory* [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**]

Parameters

coldboot
Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

directory *directory*
Specifies a fully qualified path to the directory where the firmware is located.

file *filename*
Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

host
Specifies the host by DNS name or IP address.

hostname
Specifies an IPv4 DNS host name.

host_ip_address
Specifies the host IP address. IPv4 and IPv6 addresses are supported.

manual
Performs a firmware download on the local switch.

no activate
Performs a firmware download without activation on the local switch.

nocommit
Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition. (Skips auto-commit after firmware download.)

noreboot
Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.

password *password*
Specifies the account password.

user *username*
Specifies the user login name for the host.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partition.

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partitionThis command supports firmware upgrades on the local switch only.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

firmware download usb

Specifies USB as the protocol used to perform a firmware download.

Syntax

firmware download usb [**coldboot**] [**noactivate**] [**nocommit**] [**noreboot**] [**manual**] **directory** *directory*

Command Default

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partition.

Parameters

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. **Caution:** Do not use this option unless instructed to do so by Brocade Technical Support.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a Top-of-Rack (ToR) switch or in a chassis with only one management module.

noactivate

Performs a firmware download without activation on the local switch.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

The device components supported by this command have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions, so the secondary partition becomes the primary partitionThis command supports firmware upgrades on the local switch only.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

To download firmware from an attached USB device using the command line:

```
switch# firmware download usb directory NOS_v5.0.0
```

firmware install

Installs new software but deletes all configuration in the system.

Parameters

ftp
Specifies FTP as the protocol used to install the firmware.

scp
Specifies SCP as the protocol used to install the firmware.

host
Specifies the host by DNS name or IP address.

host_ip_address
Specifies the host IP address. IPv4 and IPv6 addresses are supported.

user *username*
Specifies the user login name for the host.

password *password*
Specifies the account password.

directory *directory*
Specifies a fully qualified path to the directory where the firmware is located.

file *filename*
Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

[**vcs-mode** { **0** | **1** | **2** }
Specifies the VCS mode for the switch when the new firmware has been installed. If not set, the platform-dependent default VCS mode is used. Values you can select are: **0** (fabric cluster mode), **1** (logical chassis cluster mode), or **2** (standalone mode).

vcs-id *vcs_id*
Specifies the new VCS ID when the new firmware has been installed. If not set, the platform-dependent default VCS ID is used. Range is 1 to 8192.

rbridge-id *rbridge-id*
Specifies the new RBridge ID when the new firmware has been installed. If not set, the platform-dependent default RBridge ID isused. Range is 1 to 239.

manual
In a dual-MM system, if the manual option is used, after firmware install is completed on both MMs, reboot them at the same time. Otherwise, the MMs may run into configuration mismatch issue.

Modes

Privileged EXEC mode

Usage Guidelines

This command cleans the existing firmware on the system before installing the new firmware. All configurations in the system is completely lost.

By default, **firmware install** installs the firmware on both the active and standby modules. If the manual option is specified, then the firmware is installed on the local module only.

CAUTION
Do not use this command unless instructed by Brocade Technical Support.

Examples

To install new firmware, delete all existing configurations, and to specifiy the vcs mode, vcs ID and RBridge ID you want the switch to come up in:

```
switch# firmware install scp host 10.70.4.109 user fvt pass pray4green directory /buildsjc/sre/SQA/nos/
nos5.0.0/nos5.0.0_bld26 vcs-mode 1 vcs-id 6 rbridgeid 10
```

firmware recover

Recovers the previous firmware version on the switch nodes if a firmware upgrade was unsuccessful.

Syntax

firmware recover [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command undes the operation that was performed using the firmware download "noactivate" option.

If you invoke a noactivate firmware download, the firmware is loaded to the secondary node without swapping partitions. If firmware recover is executed, it will perform a forceful commit in that node. This CLI does not reboot the node.

The **rbridge-id** operand is supported in VCS mode only.

Examples

To recover firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware recover rbridge-id rid1-rid3,rid5
```

To perform a firmware recovery on all switch nodes:

```
switch# firmware recover rbridge-id all
```

Related Commands

firmware activate, show firmwaredownloadstatus, show version

firmware restore

Swaps the partition and reboots the node.

Syntax

firmware restore

Modes

Privileged EXEC mode

Usage Guidelines

CAUTION
Do not use this command unless instructed by Brocade Technical Support.

Use this command to restore the previously active firmware image. You can run this command only if auto-commit mode was disabled during the firmware download. After a firmware download and a reboot (with auto-commit mode disabled), the downloaded firmware becomes active. If you do not want to commit the firmware, use the **firmware restore** command.

This command reboots the system and reactivates the previous firmware. After reboot, all primary and secondary partitions restore the previous firmware image.

This command causes the node to boot up with its older firmware. Later, the image in the primary partition is automatically committed to the secondary partition.

This command is supported only on the local management module.

The **firmware download** command must have been run with the **nocommit** parameter for the **firmware restore** operation to succeed.

Examples

To restore the previous firmware:

```
switch# firmware restore

Restore old image to be active ...
Restore both primary and secondary image after reboot.
The system is going down for reboot NOW !!
Broadcast message from root (ttyS0) Fri Oct 26 23:48:54 2001...
Doing firmwarecommit now.
Please wait ...
```

Related Commands

firmware commit, firmware download, show version

firmware sync

Synchronizes the firmware on the current switch to the standby Management Module (MM).

Syntax

firmware sync

Modes

Privileged EXEC mode

Examples

To install new firmware, delete all existing configurations, and to specifiy the vcs mode, vcs ID and RBridge ID you want the switch to come up in:

```
switch# firmware sync

This command will approximately take 15 minutes to complete.

It will cause the standby MM to reboot during the process. All CLIs on active MM
in this login session will be blocked until the process is complete.

Do you want to continue? [y/n]:y
```

flexport

Used in conjunction with the **hardware** command to set the switch into FlexPort configuration mode.

Syntax

flexport *rbridge-id/slot/port* [**:***breakout-index*]

Parameters

rbridge-id/slot/port

Specifies a valid Fibre Channel port interface.

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

port

Specifies which port to modify.

:*breakout-index*

Specifies which port to modify.

Usage Guidelines

Refer to hardware on page 461.

Modes

Hardware configuration mode

Examples

This command configures connector group 5 on Rbridge ID 1.

```
switch# configure terminal
switch(config)# hardware
switch(config-hw)# flexport 1/0/5
switch(conf-hw-flex-1/0/5)#
```

This command configures connector group 5 on Rbridge ID 1.

```
switch# configure terminal
switch(config)# hardware
switch(config-hw)# flexport 1/0/5
switch(conf-hw-flex-1/0/5)#
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

connector-group, hardware, speed (FlexPort)

forward-delay

Specifies the time an interface spends in each of the listening and learning states.

Syntax

forward-delay *seconds*

no forward-delay

Command Default

15 seconds

Parameters

seconds

Specifies the time that an interface spends in the Spanning Tree Protocol (STP) learning and listening states. Valid values range from 4 through 30 seconds.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

This command specifies how long the listening and learning states last before the interface begins the forwarding of all spanning-tree instances.

STP interface states:

- Listening - The interface processes the Bridge Protocol Data Units (BPDUs) and awaits possible new information that might cause it to return to the blocking state.
- Learning - The interface does not yet forward frames (packets), instead it learns source addresses from frames received and adds them to the filtering database (switching database).
- Forwarding - An interface receiving and sending data, normal operation. STP still monitors incoming BPDUs that can indicate it should return to the blocking state to prevent a loop.
- Blocking - An interface that can cause a switching loop, no user data is sent or received, but it might go to the forwarding state if the other links in use fail and the STP determines that the interface may transition to the forwarding state. BPDU data continues to be received in the blocking state.

When you change the spanning-tree forward-delay time, it affects all spanning-tree instances. When configuring the forward-delay, the following relationship should be kept:

2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Enter **no forward-delay** to return to the default settings.

Examples

To configure the forward-delay time to 18 seconds:

```
switch(conf-mstp)# forward-delay 18
```

Related Commands

hello-time, max-age

gateway-address

Configures the gateway IP address for IPv4 or IPv6 Fabric-Virtual-Gateway sessions.

Syntax

gateway-address *gateway-address*

no gateway-address *gateway-address*

Command Default

None

Parameters

gateway-address

IPv4 or IPv6 address in the format A.B.C.D/L or x:x:x:x::x/L.

Modes

IPv4 or IPv6 Fabric-Virtual-Gateway on a VE interface configuration mode

Usage Guidelines

Enter the **no** form of the command to remove the gateway IP address for the IPv4 or IPv6 Fabric-Virtual-Gateway from the RBridge VE interface mode.

Examples

The following example shows how to configure the the gateway IP address for IPv4 Fabric-Virtual-Gateway on the VE interface.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ip fabric-virtual-gateway
switch(config-ip-fabric-virtual-gw)# gateway-address 192.128.2.1/24
```

The following example shows how to configure the gateway IP address for IPv6 Fabric-Virtual-Gateway on the VE interface.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ipv6 fabric-virtual-gateway
switch(config-ipv6-fabric-virtual-gw)# gateway-address 2001:1:0:1::1/64
```

History

Release version	Command history
5.0.1	This command was introduced.

gateway-mac-address

Configures the gateway MAC address for IPv4 or IPv6 Fabric-Virtual-Gateway sessions.

Syntax

gateway-mac-address *mac-address*

no gateway-mac-address

Command Default

Default gateway MAC address for IPv4 is **02e0.5200.010f** and for IPv6 is **02e0.5200.020e.**

Parameters

mac-address

Gateway MAC address in HHHH.HHHH.HHHH format.

Modes

Address-family configuration mode

Usage Guidelines

Enter the **no** form of the command to remove a gateway MAC address for the IPv4 or IPv6 Fabric-Virtual-Gateway session.

Examples

The following example shows how to configure the gateway MAC address for an IPv4 Fabric-Virtual-Gateway session.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv4
switch(conf-address-family-ipv4)# gateway-mac-address 0011.2222.2233
```

History

Release version	Command history
5.0.1	This command was introduced.

graceful-restart (BGP)

Enables the BGP graceful restart capability.

Syntax

graceful-restart [**purge-time** *seconds* | **restart-time** *seconds* | **stale-routes-time** *seconds*]

no graceful-restart

Command Default

Disabled

Parameters

purge-time

Specifies the maximum period of time, in seconds, for which a restarting device maintains stale routes in the BGP routing table before purging them. The default value is 600 seconds. The configurable range of values is from 1 to 3600 seconds.

restart-time

Specifies the restart-time, in seconds, advertised to graceful restart-capable neighbors. The default value is 120 seconds. The configurable range of values is from 1 to 3600 seconds.

stale-routes-time

stale-routes-time Specifies the maximum period of time, in seconds, that a helper device will wait for an EOR message from a peer. All stale paths are deleted when this time period expires. The default value is 360 seconds. The configurable range of values is from 1 to 3600 seconds.

Modes

BGP address-family IPv4 unicast configuration mode.

BGP address-family IPv6 unicast configuration mode.

Usage Guidelines

Use the no form of this command to disable the BGP graceful restart capability globally for all BGP neighbors.

Use this command to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. If the graceful restart capability is enabled after a BGP session has been established, the neighbor session must be cleared for GR to take effect.

The **purge-time** parameter is applicable for both restarting and helper devices. The timer starts when a BGP connection is closed. The timer ends when an EOR is received from all nodes, downloaded into BGP and an EOR sent to all neighbors. The configured purge-time timer value is effective only on the configured node.

The **restart-time** parameter is applicable only for helper devices. The timer starts at the time the BGP Connection is closed by the remote peer and ends when the Peer connection is established. The configured restart-time timer value is effective only on the peer node, and not in the configured node. During negotiation time, the timer value is exchanged.

The **stale-routes-time** parameter is applicable only for helper devices. The timer starts when the peer connection is established once the ha-failover peer node has been established. The timer ends at the time an EOR is received from the peer. The configured stale-time timer value is effective only on the configured node.

Use the **clear ip bgp neighbor** command with the **all** parameter for the changes to the GR parameters to take effect immediately.

Examples

To enable the BGP graceful restart capability.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
```

To set the purge time to 240 seconds.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart purge-time 240
```

To set the restart time to 60 seconds.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart restart-time 60
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

To set the stale-routes time to 180 seconds.

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv6u)# graceful-restart stale-routes-time 180
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

History

Release version	Command history
5.0.0	This command was introduced.

graceful-restart (OSPF)

Enables the OSPF Graceful Restart (GR) capability.

Syntax

graceful-restart [**helper-disable** | **restart-time** *seconds*]

no graceful-restart

Command Default

Graceful restart and graceful restart helper capabilities are enabled.

Parameters

helper-disable

Disables the GR helper capability.

restart-time

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 to 1800 seconds.

Modes

OSPF VRF router configuration mode.

Usage Guidelines

Use **no graceful-restart** to disable the graceful restart capability.

Use **no graceful-restart helper-disable** to re-enable the GR helper capability.

Examples

To disable the GR capability.

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router ospf
switch(config-router-ospf-vrf-default-vrf)# no graceful-restart
```

To disable the GR helper capability.

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router ospf
switch(config-router-ospf-vrf-default-vrf)# graceful-restart helper-disable
```

To re-enable the GR helper capability.

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router ospf
switch(config-router-ospf-vrf-default-vrf)# no graceful-restart helper-disable
```

To re-enable the GR capability.

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router ospf
switch(config-router-ospf-vrf-default-vrf)# graceful-restart
```

To re-enable the GR capability and change the maximum restart wait time from the default value to 240 seconds.

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router ospf
switch(config-router-ospf-vrf-default-vrf)# graceful-restart restart-time 240
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

graceful-restart helper (OSPFv3), nonstop-routing

graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

Syntax

graceful-restart helper { **disable** | **strict-lsa-checking** }

no graceful-restart helper

Command Default

GR helper is enabled.

Parameters

disable

Disables the OSPFv3 GR helper capability.

strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no graceful-restart helper** to disable the GR helper capability on a device.

Examples

To enable GR helper and set strict LSA checking:

```
switch# configure
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 router ospf
switch(config-ipv6-router-ospf-vrf-default-vrf)# graceful-restart helper strict-lsa-checking
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

graceful-restart (OSPF), nonstop-routing

gratuitous-arp timer

Configures the global gratuitous ARP timer in VCS.

Syntax

gratuitous-arp timer *value*

no gratuitous-arp timer

Command Default

The gratuitous ARP timer is disabled.

Parameters

value

Gratuitous ARP timer in seconds. The range is from 0 through 360.

Modes

Fabric-Virtual-Gateway address-family IPv4 or IPv6 configuration mode

Fabric-Virtual-Gateway global interface VE IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command to remove the configured gratuitous ARP timer value.

Examples

The following example shows how to configure the gratuitous ARP timer in Fabric-Virtual-Gateway address-family IPv4 configuration mode.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv4
switch(conf-address-family-ipv4)# gratuitous-arp timer 15
```

The following example shows how to configure the gratuitous ARP timer in Fabric-Virtual-Gateway under VE interface IPv4 configuration mode.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ip fabric-virtual-gateway
switch(config-ip-fabric-virtual-gw)# gratuitous-arp timer 15
```

The following example shows how to configure the gratuitous ARP timer in Fabric-Virtual-Gateway address-family IPv6 configuration mode.

```
switch(config)# router fabric-virtual-gateway
switch(conf-router-fabric-virtual-gateway)# address-family ipv6
switch(conf-address-family-ipv6)# gratuitous-arp timer 60
```

The following example shows how to configure the gratuitous ARP timer in Fabric-Virtual-Gateway under VE interface IPv6 configuration mode.

```
switch(config)# interface ve 3000
switch(config-Ve-3000)# ipv6 fabric-virtual-gateway
switch(config-ipv6-fabric-virtual-gw)# gratuitous-arp timer 60
```

History

Release version	Command history
5.0.1	This command was introduced.

ha chassisreboot

Performs a reboot of the chassis.

Syntax

ha chassisreboot

Modes

Privileged EXEC mode

Usage Guidelines

This command reboots the entire chassis. Both the active and the standby management module reboot. Both management modules retain their original high-availability (HA) role after the system comes back up. If the power-on self test (POST) is enabled, it is executed when the system comes back up.

This command is supported only on the active management module. This command is not supported on the standby management module. Both management modules must be in sync for the HA reboot operation to succeed. Failover and reboots can be disruptive.

Examples

To perform an HA reboot:

```
switch# ha chassisreboot
```

Related Commands

ha failover, ha enable, reload, show ha

ha disable

Disables the High Availability (HA) feature on a switch.

Syntax

ha disable

Command Default

HA is disabled.

Modes

Privileged EXEC mode

Usage Guidelines

If the HA feature is already disabled, this command has no effect.

This command is supported only on the active management module.

This command is not supported on the standby management module.

Do not use this command unless instructed by Brocade Technical Support.

NOTE
With the introduction of Network OS 4.0, failover is no longer disruptive for Layer 2.

Examples

To display the syslog daemon IP addresses configured on a switch:

```
switch# ha disable

Service instances out of sync
1970/01/01-00:06:30, [HASM-1101], 111, MM1, WARNING, chassis, HA State out of sync.
HA is disabled
```

Related Commands

ha enable, reload, show ha

ha enable

Enables the High Availability (HA) feature on a switch.

Syntax

ha enable

Command Default

HA is disabled.

Modes

Privileged EXEC mode

Usage Guidelines

If the HA feature is already enabled, this command has no effect. If the HA feature is disabled, this command enables it. The standby management process reboots as part of the process

Running the command displays a warning message and prompts for confirmation before rebooting the management module.

You can also use this command to display the servers that are running the syslogd daemon and those that system messages are sent to. Servers are specified in the configuration database by IP address.

This command is supported only on the local management module.

This command is not supported on the standby management module.

Do not use this command unless instructed by Brocade Support.

NOTE
With the introduction of Network OS 4.0, failover is no longer disruptive for all Layer 2.

Examples

To display the syslog daemon IP addresses configured on a switch:

```
switch# ha enable

Warning: This command will enable the HA. It will reboot the standby CP and
require all telnet, secure telnet, and SSH sessions to the standby CP to be
restarted.
Are you sure you want to go ahead  [y/n]? y

1970/01/01-00:07:18, [EM-1047], 113, MM1, INFO, chassis, CP in slot 2 not faulty, CP ERROR deasserted.
HTBT hit a threshold: 2
HTBT hit a threshold: 2
Heartbeat to 2 Down!
 resetting peer
 resetting peer 127.2.1.2
HA is enabled
```

Related Commands

ha disable, ha failover, reload, show ha

ha failover

Initiates a failover from the active to the standby management module (MM).

Syntax

ha failover

Modes

Privileged EXEC mode

Usage Guidelines

With the introduction of Network OS 4.0, failover is no longer disruptive for all Layer 2.

This command forces a failover from the active to the standby MM. When the process completes, the former standby takes over as the active MM. If the active and standby MMs are not synchronized, the command aborts.

Examples

To perform a failover:

```
switch# ha failover
```

ha sync start

This command is used to enable the high availability (HA) state synchronization.

Syntax

ha sync start

Modes

Privileged EXEC mode

Examples

To enable HA synchronization:

```
switch# ha sync start
Are you sure you want to start sync [y/n]
All service instances in sync
2012/10/06-16:10:36, [HASM-1100], 630, M2, INFO, VDX8770-4, HA State is in sync.
```

ha sync stop

Disables high availability state synchronization on a switch.

Syntax

ha sync stop

Command Default

Synchronization is enabled.

Modes

Privileged EXEC mode

Examples

To disable state synchronization:

```
switch# ha sync stop
Are you sure you want to stop sync [y/n]? y
Service instances out of sync
2012/10/06-16:06:13, [HASM-1101], 619, M2, WARNING, VDX8770-4, HA State out of sync.
```

Related Commands

ha failover, ha enable, ha sync start

hardware

Enters hardware configuration mode to enter FlexPort and port-group configuration mode.

Syntax

hardware

Modes

Global configuration mode

Usage Guidelines

Use this command to enter hardware configuration mode. While in this mode you can enter connector configuration mode for the purpose of configuring breakout mode. You can also enter port-group configuration mode on Brocade 27x40 GbE line cards.

Examples

Typical command usage:

```
switch# configure terminal
switch(config)# hardware
switch(config-hw)#
```

Related Commands

connector-group, flexport, speed (FlexPort)

hardware-profile

Optimizes hardware resources for route profiles or ternary content-addressable memory (TCAM) profiles.

Syntax

hardware-profile { **route-table** { **default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd** } | **tcam** { **default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd** }}

Command Default

The default hardware profiles are enabled.

Parameters

route-table

Optimizes hardware resources for route profiles.

default

Optimizes IPv4/IPv6 resources for dual-stack operations.

ipv4-max-route

Optimizes resources for the maximum number of IPv4 routes.

ipv4-max-arp

Optimizes resources for the maximum number of IPv4 ARP entries.

ipv4-min-v6

Optimizes resources for IPv4 routes in dual-stack configurations.

ipv6-max-route

Optimizes resources for the maximum number of IPv6 routes.

ipv6-max-nd

Optimizes resources for the maximum number of IPv6 Neighbor Discovery entries.

tcam

Optimizes hardware resources for TCAM profiles.

default

Optimizes resources with basic support for all applications.

l2-ipv4-acl

Optimizes resources for Layer 2 and IPv4 ACLs.

ipv4-v6-pbr

Optimizes resources for IPv4 and IPv6 ACLs and policy-based routing tables.

ipv4-v6-qos

Optimizes resources for IPv4 and IPv6 ACLs and QoS.

ipv4-v6-mcast

Optimizes resources for multicast.

l2-acl-qos
Optimizes resources for Layer 2 ACLs and QoS.

Modes

RBridge ID configuration mode

Usage Guidelines

ATTENTION
This is a disruptive command. You must reload (reboot) the switch before the most recent profile takes effect. Once a profile is activated, it persists across chassis reboots. However, once a switch profile is changed, a reboot is required.

There is no **"no"** form of this command.

Examples

To optimize route profiles for IPv4/IPv6 dual-stack operations:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# hardware-profile route-table default
```

To optimize TCAM resources for multicast:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# hardware-profile tcam ipv4-v6-mcast
```

History

Release version	Command history
Network OS v5.0.0	This command was introduced.

hello-interval (ELD)

This global level configuration defines the interval for sending edge-loop detection (ELD) PDUs.

Syntax

hello-interval *milliseconds*

no hello-interval *milliseconds*

Command Default

The default value is 1000 ms (one second)

Parameters

milliseconds

Interval time in milliseconds. The range is from 100 ms through 5 seconds.

Modes

ELD configuration mode

Usage Guidelines

This command applies only in Brocade VCS Fabric mode.

It is the user's responsibility to make sure that the hello interval is set to the same value across the various VCS clouds. Otherwise, the ELD port shutdown will be non-deterministic.

Extreme caution must be taken when setting the hello-interval value to anything less than 1 second, as it will heavily increase the cpu load due to the amount of packets transmitted and received (depending on the number of ELD instances and other system configuration), and might cause undesirable performance and scalability results.

Enter **no hello-interval** *milliseconds* to return to the default setting.

Examples

To set the PDU hello-interval to 5 seconds:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# hello-interval 5000
```

To return the PDU hello-interval to the default value (1000 ms):

```
switch(config-eld)# no hello-interval 5000
```

hello (LLDP)

Sets the interval between LLDP hello messages

Syntax

hello *seconds*

no hello

Command Default

30 seconds

Parameters

seconds

Valid values range from 4 through 180 seconds.

Modes

LLDP protocol configuration mode

Usage Guidelines

Enter **no hello** to return to the default setting.

Examples

To set the time interval to 10 seconds between the transmissions:

```
switch# configure terminal
switch (config)# protocol lldp
switch(conf-lldp)# hello 10
```

hello (UDLD)

Sets the hello transmit interval.

Syntax

hello *hundred_milliseconds*

no hello

Command Default

5 is the default value (500 milliseconds).

Parameters

hundred_milliseconds

Valid values range from 1 through 60 (in counts of 100 milliseconds).

Modes

Unidirectional link detection (UDLD) protocol configuration mode

Usage Guidelines

Use this command to set the time interval between the transmission of hello UDLD PDUs from UDLD-enabled ports.

Enter **no hello** to return to the default setting.

Examples

To set the time interval to 2,000 milliseconds between hello UDLD PDU transmissions:

```
switch# configure
switch (config)# protocol udld

switch(config-udld)# hello 20
```

Related Commands

multiplier (UDLD), protocol udld

hello-interval

Sets the interval between PDU packets sent from the ELD-enabled edge ports of a Brocade VCS Fabric cluster.

Syntax

hello-interval *interval*

no hello-interval

Command Default

1000 (one second)

Parameters

interval

Number of periods between each PDU. For example, a value of 2000 causes a PDU to be sent every two seconds. Valid values range from 100 through 5000 milliseconds (100 ms through 5 seconds).

Modes

ELD configuration mode

Usage Guidelines

Use this command with the **pdu-rx-limit** command to determine the time taken to detect a loop. The time taken to detect a loop is the product of the pdu-rx-limit and the hello interval.

The hello interval must be set to the same value on all Brocade VCS Fabric clusters that have ELD enabled, otherwise it cannot be predicted which Brocade VCS Fabric cluster will reach its limit first. The Brocade VCS Fabric cluster in the loop with the lowest pdu-rx-limit is the cluster where the loop gets broken, assuming that the hello interval is correctly set to the same value on all clusters.

This command applies only in Brocade VCS Fabric mode.

This functionality detects Layer 2 loops only.

Enter **no hello-interval** to return to the default setting.

CAUTION

Use extreme caution when setting the hello interval value to less than 1 second because it heavily increases the CPU load due to the number of packets transmitted and received. This load depends on the number of ELD instances and other system configuration parameters. Undesirable performance and scalability might occur.

Examples

To set the PDU interval to 5 seconds:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# hello-interval 5000
```

To reset the PDU interval to its default value of 1 second:

```
switch(cfg-eld)# no hello-interval 5000
```

Related Commands

pdu-rx-limit, protocol edge-loop-detection, show edge-loop-detection globals

hello-time

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent on an interface.

Syntax

hello-time *seconds*

no hello-time

Command Default

2 seconds

Parameters

seconds

Specifies the time interval between the hello BPDUs sent on an interface. Valid values range from 1 through 10 seconds.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

This command configures the spanning-tree bridge hello time, which determines how often the device broadcasts hello messages to other devices.

If the VLAN parameter is not provided, the hello-time value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration. When configuring the **hello-time**, the **max-age** command setting must be greater than the **hello-time** setting. The following relationship should be kept:

```
2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)
```

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Enter **no hello-time** to return to the default settings.

To configure spanning-tree bridge hello time to 5 seconds:

```
switch(conf-stp)# hello-time 5
```

Related Commands

forward-delay, max-age

hello-timer

Configures the Hello message periodic interval.

Syntax

hello-timer *num*

no hello-timer

Command Default

30 seconds

Parameters

num

The interval value in seconds. Valid values range from 10 through 3600 seconds.

Modes

PIM router configuration mode

Usage Guidelines

This command specifies the interval between Protocol Independent Multicast (PIM) "Hello" messages.Enter **no hello-timer** to return to the default settings.

Examples

Setting the hello-timer to 60 seconds.

```
switch(conf-pim-router)# hello-timer 60
```

Related Commands

router pim

hold-time

Sets the time that a previously down backup VRRP router, which also must have a higher priority than the current master VRRP router, will wait before assuming mastership of the virtual router.

Syntax

hold-time *range*

Command Default

0 seconds

Parameters

range

A value between 1 and 3600 seconds that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The hold-time must be set to a number greater than the default of 0 seconds for this command to take effect.

This command can be used for both VRRP and VRRP-E.

Examples

To set the hold time to 60 seconds for backup routers in a specific virtual router:

```
switch(config)# rbridge-id 101

switch(config-rbridge-id-101)# int ve 25

switch(config-ve-25)# vrrp-extended-group 1

switch(config-vrrp-extended-group-1)# hold-time 60
```

Related Commands

vrrp-group

hold-time (Fabric-Virtual-Gateway)

Configures the duration for which the Fabric-Virtual-Gateway session will remain idle before activating the configuration on the system.

Syntax

hold-time *hold-time*

no hold-time

Command Default

None

Parameters

hold-time

The hold time in seconds.

Modes

Fabric-Virtual-Gateway under VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command to remove the hold-time duration for the IPv4 or IPv6 Fabric-Virtual-Gateway configuration.

Examples

The following example shows how to configure the hold time.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ip fabric-virtual-gateway
switch(config-ip-fabric-virtual-gw)# hold-time 30
```

History

Release version	Command history
5.0.1	This command was introduced.

http server shutdown

Disables or enables an HTTP server.

Syntax

http server shutdown

no http server shutdown

Modes

Global configuration mode

Usage Guidelines

Use the **http server shutdown** command to disable an HTTP server. All active connections are closed and the Apache httpd server process does not run.

Use the **no http server shutdown** command to enable an HTTP server. This restarts the Apache httpd server process, which starts listening for HTTP requests.

ATTENTION
You cannot downgrade directly to a previous Network OS release with the HTTP server disabled. You must first execute the **no http server shutdown** command and then downgrade.

Examples

To disable an HTTP server:

```
switch(config)# http server shutdown
```

To enable an HTTP server:

```
switch(config)# no http server shutdown
```

inactivity-timer

Configures the forwarding entry inactivity timer.

Syntax

inactivity-timer *num*

no inactivity-timer

Command Default

180 seconds

Parameters

num

The entry inactivity timer interval. Valid values range from 60 through 3600 seconds.

Modes

PIM router configuration mode

Usage Guidelines

This command to specifies the delay interval until a forwarding entry is considered to be active. At the expiration of this timer, the router deletes a forwarding entry.

Enter **no inactivity-timer** to return to the default setting.

Examples

To set the timer to 600 seconds.

```
switch(conf-pim-router)# inactivity-timer 600
```

Related Commands

router pim

install-igp-cost

Configures the device to use the IGP cost instead of the default BGP4or BGP4+ Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

Syntax

install-igp-cost

no install-igp-cost

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

By default, BGP4or BGP4+ use the BGP MED value as the route cost when the route is added to the RTM. Use this command to change the default to the IGP cost

Use the **no** form of this command to restore the default.

Examples

To configure the device to compare MEDs:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# install-igp-cost
```

instance

Maps a VLAN to a Multiple Spanning Tree Protocol (MSTP) instance. You can group a set of VLANs to an instance.

Syntax

instance *instance_id* [**vlan** *vlan_id* | **priority** *priority_id*]

no instance

Command Default

The priority value is 32768.

Parameters

instance_id

Specifies the MSTP instance. Valid values range from 1 through 31.

vlan *vlan_id*

Specifies the VLAN to map an MSTP instance. Refer to the Usage Guidelines.

priority *priority_id*

Specifies the priority for the specified instance. Valid values range from 0 through 61440. The priority values can be set only in increments of 4096.

Modes

Protocol Spanning Tree MSTP configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

See "User-configurable VLAN IDs" on page 11.

The following rules apply:

- VLANs must be created before mapping to instances.
- VLAN instance mapping is removed from the configuration if the underlying VLANs are deleted.

Enter **no instance** to un-map the VLAN from the MSTP instance.

CAUTION
This command can be used only after the VLAN is defined.

Examples

To map a VLAN to an MTSP instance:

```
switch(conf-mstp)# instance 1 vlan 2,3
switch(conf-mstp)# instance 2 vlan 4-6
switch(conf-mstp)# instance 1 priority 4096
```

Related Commands

show spanning-tree

interface

Enters the interface configuration mode to configure an interface.

Syntax

interface [**fibrechannel** *rbridge-id/slot/port* | **fcoe** *vn-number/rbridge-id/front-port-number* | *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **vlan** *vlan_id*]

no interface [**port-channel** *number* | **vlan** *vlan_id* | **fcoe** *vn-number/rbridge-id/front-port-number*]

Parameters

fibrechannel *rbridge-id/slot/port*
Specifies a valid Fibre Channel port interface (Brocade VDX 6740 switches only in Brocade VCS Fabric mode).

rbridge-id
Specifies the RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

fcoe *vn-number/rbridge-id/front-port-number*
Specifies a valid FCoE port interface.

vn-number
Specifies the VN number for FCoE.

rbridge-id
Specifies the routing bridge ID.

front-port-number
Specifies the front port number.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies the port-channel number. The number of available channels ranges from 1 through 6144.

vlan *vlan_id*
Specifies the VLAN number. Refer to the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Enter **no interface** followed by the appropriate interface identification parameters to disable that interface.

Examples

To configure a Fibre Channel port on a Brocade VDX 6740 switch:

```
switch(config)# interface FibreChannel 66/0/1
switch(config-FibreChannel-66/0/1)#
```

To enter FCoE configuration mode for an interface:

```
switch(config)# interface fcoe 1/0/1
switch(config-Fcoe-1/0/1)#
```

To enter configuration mode on a 1 Gbps interface on a Brocade VDX switch:

```
switch(config)# interface gigabitethernet 1/0/1
switch(config-if-gi-1/0/1)#
```

Related Commands

interface management, interface ve, interface vlan, show interface

interface (range specification)

Allows a range of values to be entered for some interface configurations.

Syntax

interface { **fibrechannel** *rbridge-id/slot/port* | **fcoe** *vn-number/rbridge-id/front-port-number* | <*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **vlan** *vlan_id* | **loopback** *port_number* | **ve** *vlan_id* }

no interface { **port-channel** *number* | **vlan** *vlan_id* | **fcoe** *vn-number/rbridge-id/front-port-number* }

Parameters

fibrechannel *rbridge-id/slot/port*

Specifies a valid Fibre Channel port interface (Brocade VDX 6740 switches only in Brocade VCS Fabric mode).

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

fcoe *vn-number/rbridge-id/front-port-number*

Specifies a valid FCoE port interface.

vn-number

Specifies the VN number for FCoE.

rbridge-id

Specifies the routing bridge ID.

front-port-number

Specifies the front port number.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the port-channel number. The number of available channels range from 1 through 6144.

vlan *vlan_id*

Specifies the VLAN number. (Refer to the Usage Guidelines.)

loopback *port_number*
Specifies the port number for the loopback interface. The range is 1 through 255.

ve *vlan_id*
Specifies the corresponding VLAN interface that must already be configured before the VE interface can be created. (Refer to the Usage Guidelines.)

Modes

Global configuration mode (Refer to the Usage Guidelines.)

Usage Guidelines

Use this command to create or enter the interface configuration mode for an interface or range of interfaces.

Loopback and VE configurations are node specific (local) in fabric custer and logical chassis cluster modes. The other interfaces that support the use of ranges work the same as shown for VLAN in the examples, except for the following differences:

VE and loopback interfaces also support ranges in RBridge configuration mode.

For example, if you want to create and/or enter VLAN interface configuration mode for VLAN IDs 3 through 8 and VLAN 10 and 12, you would enter the following command in global configuration mode:

```
switch(config)# interface vlan 3-8,10,12
```

NOTE
Do not use a space after a comma or you will receive a syntax error.

You then receive the following prompt:

```
switch(config-Vlan-3-8,10,12)#
```

Any command you run from this prompt takes effect on all VLANs that you have specified.

You can use the **no** form of commands on ranges in the same way. For example, if you want to remove the description on VLANS 10 through 15 and VLAN 19 all at the same time, you would enter the following commands in global configuration mode:

```
switch(config)# interface vlan 10-15,19
switch(config-vlan-10-15,19)# no description
```

NOTE
The **no** form of the command for deleting interfaces should not be given from the range sub-mode. Exit the range sub-mode before deleting interfaces.

The three gigabit interface types have the following restrictions for range specification in VCS mode:

- Ranges cannot be used for interfaces that belong to multiple slots. However, you can configure a range of interfaces if each interface in the range belongs to the same slot.
- Ranges can be applied only to interfaces that belong to the same RBridge.

Fibrechannel interfaces have the following restrictions for range specification in VCS mode:

- Ranges cannot be used for interfaces that belong to multiple slots. However, you can configure a range of interfaces if each interface in the range belongs to the same slot.
- Ranges can be applied only to interfaces that belong to the same RBridge.

For the fibre channel interface, ranges can be applied only to interfaces that belong to the same RBridge.

An FCoE interface from one node cannot be combined with a bind configuration of a physical port/port-channel that belongs to another node in the cluster. Refer to the Examples.

A set of FCoE ports cannot be bound to the same MAC address.

Examples

Examples

To configure binding between a range of FCoE ports (0 to 20 in this example) to the tengigabitethernet port 10/0/1:

```
switch# configure
switch(config)# interface Fcoe 1/10/0 - 1/10/20
sw0(conf-Fcoe-1/10/0-20) bind te 10/0/1
```

The FCoE interfaces and the bind configuration of the physical port/port-channel must belong to the same node in the cluster. An example of an unsupported configuration is:

```
switch# configure
switch(config)# interface Fcoe 1/10/0 - 1/10/20
sw0(conf-Fcoe-1/10/0-20)# bind te 20/0/1
```

Examples

To enter interface subtype configuration mode on a tengigabitethernet interface with an RBridge ID of 25 and a slot of 0, with a port range of 1 through 10, 17 through 21, and 24:

```
sw0(config)# interface TenGigabitEthernet 25/0/1-10,17-21,24
sw0(conf-if-te-25/0/1-10,17-21,24)#
```

interface loopback

Configures a loopback interface.

Syntax

interface loopback *port_number*

no interface loopback *port_number*

Command Default

A loopback interface is not configured.

Parameters

port_number

Specifies the port number for the loopback interface. The range is 1 through 255.

Modes

RBridge ID configuration mode (for VCS)

Usage Guidelines

A loopback is a logical interface traditionally used to ensure stable routing operations.

The following restrictions apply when the loopback interface is part of an active XVLAN overlay gateway. These restrictions are enforced to maintain consistency across the gateway.

- The loopback interface cannot be deleted.
- The IPv4 address cannot be changed.
- The VRF instance cannot be changed.

You must first use the **no activate** command in VXLAN overlay gateway configuration mode to modify the loopback interfaces. .

Use the no form of this command with a port parameter to remove the specified loopback interface.

Examples

The following example creates a loopback interface with a port number of 25 for RBridge ID 11. The command is executed in a VCS environment.

```
switch(config)# rbridge-id 11
switch(config-rbridge-id-11)# interface loopback 25
```

interface management

Enters configuration mode for the management interface. Also used for binding ACLs to a management interface.

Syntax

interface management *rbridge-id/port*

Command Default

DHCP is disabled.

IPv6 stateless auto-configuration is disabled.

The speed setting is **auto**.

Parameters

rbridge-id/port

Specifies the management interface to be configured as the *rbridge-id* followed by a slash (/) and the port number.

port

On Top-of-Rack (ToR) switches, the port number for the management port is always 0. On a modular switches with two redundant management modules, can configure two management ports: 1 and 2.

Modes

Global configuration mode

Usage Guidelines

This command supports IP addresses in IPv6 and IPv4 format. This command enters a management interface configuration mode where you can choose configuration parameters for IPv4 and IPv6 addresses.

Once you have executed this command, the following commands become available to configure the management interface:

- **ip address**
- **ip access-group**
- **ip gateway-address**
- **ip route**
- **ipv6 address**
- **ipv6 access-group**
- **speed**

The **ip gateway-address** command will not be available on the Brocade VDX series if the Layer 3 or Advanced Services license is installed. In that case, use the following command sequence:

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# ip route 0000/0 <default_gateway_address>
```

Setting a static IPv4 address and DHCP are mutually exclusive. If DHCP is enabled, you must disable DHCP before you can configure a static IPv4 address.

A static IPv6 address and stateless auto-configuration can coexist.

Auto-configuration is configured chassis-wide and you configure it always under **interface management** *rbridge-id/1*. Once the feature is configured under **interface management** *rbridge-id/1* it is configured for both management interfaces.

Enter **no ip address** *ipv4_address/prefix_len* **dhcp** to disable DHCP. For other operands, use the **no** form of the command to remove the corresponding configuration.

Enter **no speed** to restore speed parameters to their defaults.

Examples

To configure a management interface with an IPv6 IP address:

```
switch(config)# interface management 1/0
switch(config-Management-1/0)# ipv6 address fd00:60:69bc:832:e61f:13ff:fe67:4b94/64
```

To set the interface to 100-Mbps Full Duplex

```
switch(config-Management-1/0)# speed 100
```

To apply an ACL to the management interfaces on a Brocade VDX 8770-4:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ip access-group stdACL3 in
switch(config-Management-1/1)# ipv6 access-group stdV6ACL1 in
switch(config-Management-1/1)# exit
switch(config)# interface Management 1/2
switch(config-Management-1/2)# ip access-group extdACL5 in
switch(config-Management-1/2)# exit
```

To enable DHCP for IPv4 addresses:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ip address dhcp
```

To enable DHCP for IPv6 addresses:

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ipv6 address dhcp
```

Applying an ACL on management interface 1/1:

```
switch(config)# interface management
switch(config)# interface management 1/1
Entering configuration mode terminal
switch(config-Management-1/1)# ip access-group stdACL1 in
```

Related Commands

interface, show interface management, show running-config interface management

interface ve

Configures a Virtual Ethernet (VE) interface.

Syntax

interface ve *vlan_id*

no interface ve *vlan_id*

Parameters

vlan_id

Specifies the corresponding VLAN interface that must already be configured before the VE interface can be created. Refer to the Usage Guidelines.

Modes

RBridge ID configuration mode (for VCS)

Global configuration mode

Usage Guidelines

Before you can configure a VE interface, you must configure a VLAN interface. The corresponding VE interface must use the same VLAN ID you used to configure the VLAN.

Use the **no** form of the command to remove the VE interface.

CAUTION
If no RBridge ID is configured on the switch, deleting the VE interface will cause a spike in CPU usage. To prevent this, configure an RBridge ID before deleting the VE interface.

Examples

The following example shows the steps needed to create a VE interface with the VLAN ID of 56 for RBridge ID 11. This example is for a VCS environment, and assumes that the VLAN 56 interface has already been created.

```
switch(config)# rbridge-id 11
switch(config-rbridge-id-11)# interface ve 56
```

The following example shows the steps needed to create a VE interface with the VLAN ID of 4093.

```
switch# configure
switch(config)# interface ve 4093
```

Related Commands

interface, interface vlan

interface vlan

Allows the user to create 802.1Q VLANs, as well as service or transport VFs in a Virtual Fabrics context.

Syntax

interface vlan *vlan_id*

no interface vlan *vlan_id*

Command Default

VLAN 1 is predefined on the switch.

Parameters

vlan_id

Specifies the VLAN interface to configure. The range is from 1 through 8191. (Refer to the Usage Guidelines.)

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a VLAN interface. This command applies to both 802.1Q VLANS (whose VLAN IDs range from 1 through 4095) and service or transport VFs (whose VLAN IDs range from 4096 through 8191).To support multitenancy, assigning VLAN IDs from 4096 through 8191 creates service or transport VFs that are unique within a local VCS Fabric but that cannot extend to another VCS Fabric.

All of the ports on the switch are a part of the default VLAN 1.

Make sure your converged mode interface is not configured to classify untagged packets to the same VLAN as the incoming VLAN-tagged packets. By configuring a converged interface to classify untagged packets (by using classifiers or the default port *vlan_id*) to the same VLAN as VLAN-tagged packets coming into the interface, the FCoE hardware sends out untagged packets to the CNA. These packets may be dropped, disrupting communications.

For service or transport VFs to be implemented in a Virtual Fabrics context, the user must execute the **vcs virtual-fabric enable** command in global configuration mode.

Enter **no interface vlan** *vlan_id* to delete a VLAN interface. This will also delete the corresponding virtual Ethernet (VE) interface.

Examples

To create a VLAN with an ID of 56:

```
switch(config)# interface vlan 56
switch(conf-if-vl-56)#
```

To create a classified VLAN (with an ID from 4096 through 8191):

```
switch(config)# interface vlan 5000
switch(conf-if-vl-5000)#
```

ip access-group

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ip access-group *ACLname* { **in** | **out** }

no ip access-group *ACLname* { **in** | **out** }

Parameters

ACLname
Specifies the name of the standard or extended IP access list.

in | **out**
Specifies the binding direction (ingress or egress).

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv4 ACL to one of the following interface types:

- User interfaces
  - Physical interfaces (<N>-gigabit Ethernet)
  - Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- All supported management interfaces
- Overlay gateways

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL
- One egress MAC ACL
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL
- One egress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of three ACLs to an overlay gateway, as follows:

- One ingress MAC ACL
- One ingress IPv4 ACL

- One ingress IPv6 ACL

  NOTE
  You can apply an ACL to multiple interfaces, and you can apply an extended ACL twice—ingress and egress—to a given user interface.

To remove an IPv4 ACL from an interface, enter **no ip access-group** *ACLname*

To remove an ACL from an interface, use the **no** form of this command.

Examples

To apply an ingress IP ACL named ipacl2 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip access-group ipacl2 in
```

To remove an ingress IP ACL named ipacl2 from a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no ip access-group ipacl2 in
```

Related Commands

interface, interface ve, ip access-list, resequence access-list

ip access-list

Creates a standard or extended IPv4 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ip access-list { **standard** | **extended** } *ACLname*

no ip access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:

standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

On any given switch, an ACL name must be unique among all ACL types (MAC/IPv4/IPv6; standard or extended).

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after if is applied to an interface, using the **access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv4 standard ACL:

```
switch# configure
switch(config)# ip access-list standard stdACL3
```

The following example creates an IPv4 extended ACL:

```
switch# configure
switch(config)# ip access-list extended extdACL5
```

The following example creates rules on an IPv4 standard ACL:

```
switch# configure
switch(config)# ip access-list standard stdACL3
switch(config-ipacl-std)# seq 5 permit host 10.20.33.4
switch(config-ipacl-std)# seq 15 deny any
```

The following example deletes an IPv4 ACL:

```
switch# configure
switch(config)# no ip access-list standard stdACL3
```

ip address

Configures an IP address.

Syntax

ip address *ip-address/mask* [**secondary**] [{ **ospf-ignore** | **ospf-active** }]

no ip address

Parameters

ip-address
IP address.

mask
Mask for the associated IP subnet. Valid values range from integers from 1 through 31. Dotted-decimal is not supported.

secondary
Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

ospf-ignore
Disables adjacency formation with OSPF neighbors and advertisement of the interface to OSPF.

ospf-passive
Disables adjacency formation with OSPF neighbors but does not disable advertisement of the interface to OSPF.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to configure a primary or secondary IP address for a specific interface. You can also use this command to prevent OSPF from running on specified subnets.Multiple primary IP addresses are supported on an interface.

A primary IP address cannot overlap with a previously configured IP subnet.

A primary IP address must configured before you configure a secondary IP address in the same subnet.

Enter **no ip address** to remove the configured static or DHCP address, resetting the address to 0.0.0.0/0.

Examples

To configure a primary IP address on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9

switch(conf-if-te-178/0/9)# ip address 1.1.1.1/24
```

To configure a secondary IP address on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# ip address 1.1.1.1/28 secondary
```

Related Commands

interface (range specification), interface ve

ip address (NSX controller configuration)

Configures the IP address, port and connection method settings for an NSX controller connection profile.

Syntax

ip address *ip-address* [**method** { **ssl** | **tcp** }] [**port** *port_number*]

Parameters

ip address *ip-address*

IP address of the NSX Controller cluster. Only IPv4 addresses are allowed. This address is used to open a connection to the NSX Controller for Open vSwitch Database Management Protocol (OVSDB) exchange.

method

Specifies the connection method for this profile.

ssl

Specifies that a Secure Sockets Layer connection will be used. This is the default connection method.

tcp

Specifies that a transmission control protocol will be used.

port *port_number*

Specifies the port number for the NSX controller. The range is 1-65535. The default 6632.

Modes

NSX controller configuration mode

Usage Guidelines

This command is allowed for a switch that is in logical chassis cluster mode only.

The VXLAN gateway must be in shutdown state.

Examples

The following example shows how to enter NSX controller configuration mode for the already created NSX controller connection profile called profile1, then how to create the IP address, set the method to TCP, and designate the port of 25:

```
switch# configuration
switch(config)# nsx-controller profile1
switch(config-nsx-controller-profile1)# ip address 10.21.83.188 method tcp port 25
```

ip address (VXLAN)

Specifies the destination IPv4 address of a tunnel in VXLAN overlay gateway configurations.

Syntax

ip address *IPv4_address*

no ip address [*IPv4_address*]

Parameters

IPv4_address
IPv4 address of the destination tunnel.

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

This command creates a tunnel when the parent overlay gateway is attached to one or more RBridges. The tunnel mode and the source IP address are derived from the parent overlay gateway.

To change an IP addresses, you must first remove the existing address, by means of the **no ip address** *IPv4_address* or the **no ip address** commands. This also deletes all tunnels to the site.

Only one IPv4 address is allowed. The following IPv4 addresses are not allowed:

- Broadcast addresses (0.0.0.0 through 0.255.255.255)
- Localhost loopback addresses (127.0.0.0 through 127.255.255.255)
- Multicast addresses (224.0.0.0 through 239.255.255.255)
- Reserved addresses (240.0.0.0 through 255.255.,255.255)

Examples

To specify an IPv4 address of a destination tunnel:

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-overlay-gw-gateway1-site-mysite)# ip address 10.11.12.13
```

Related Commands

overlay-gateway, site

ip arp-aging-timeout

Sets how long an ARP entry stays in cache before the cache refreshes.

Syntax

ip arp-aging-timeout *value*

no ip arp-aging-timeout

Command Default

ip arp-aging-timeout is enabled and set to 240 minutes.

Parameters

value

Determines how long an ARP entry stays in cache. For 1-gigabit, 10-gigabit, 40-gigabit, and Virtual Ethernet interfaces, the range of valid values is from 0 through 240 minutes.

Modes

Interface subtype configuration mode

Usage Guidelines

When a Brocade device places an entry in the ARP cache, the device also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The ARP age affects dynamic (learned) entries only, not static entries.

Enter **no ip arp-aging-timeout** command to disable aging so that entries do not age out.

Entering **ip arp-aging-timeout 0** also disables aging.

Examples

To set the IP ARP aging timeout value to 100 minutes for a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip arp-aging-timeout 100
```

To disable IP ARP aging for a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip arp-aging-timeout
```

Related Commands

interface, interface ve

ip as-path access-list

Configures an AS-path access control list (ACL), specifies the community name, and whether to permit or deny traffic.

Syntax

ip as-path access-list *string* [**seq** *seq-value*] [**deny** *regular-expression* | **permit** *regular-expression*]

no ip as-path access-list *string* [**seq** *seq-value*] [**deny** *regular-expression* | **permit** *regular-expression*]

Command Default

This option is disabled.

Parameters

string
ACL name.

seq-value
Sequence number as defined by the **seq** command.

regular-expression
A string inside quotes.

Modes

RBridge ID configuration mode

Usage Guidelines

This command accepts a regular expression that must be enclosed in quotes.

Use the **no** form of this command to restore the default.

Examples

To create an AS-path ACL:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip as-path access-list seq 10 permit "myaspath"
```

Related Commands

seq (IPv6 extended ACLs), seq (IPv6 standard ACLs)

ip community-list extended

Configures a community access control list (ACL), specifies the community name, and whether to permit or deny traffic, including through the use of a regular expression.

Syntax

ip community-list extended *community-list-name* { **deny** *string* | **permit** *string* } [**seq** *seq*] [**internet** | **local-as** | **no-advertise** | **no-export**]

no ip community-list extended *community-list-name*

Command Default

This option is disabled.

Parameters

community-list-name
Range is from 1 through 32 ASCII characters.

string
An ordered community-list regular expression.

seq
Sequence number. Range is from 1 through 65535.

internet
The Internet community.

no-export
Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGP neighbors.

local-as
Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.

no-advertise
Routes with this community cannot be advertised to any other BGP4 devices at all.

regular-expression
A string enclosed in quotes.

Modes

RBridge ID configuration mode

Usage Guidelines

Unlike a standard community list, this command does accept a regular expression as long as the string is enclosed in quotes.

Use the **no** form of this command to restore the default.

Examples

To create an extended community list:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip community-list extended seq 10 permit "mycommunity"
```

Related Commands

ip community-list standard, seq (IPv6 extended ACLs)

ip community-list standard

Configures a community access control list (ACL), specifies the community number or type, and whether to permit or deny traffic.

Syntax

ip community-list standard *community-list-name* { **deny** [*community-number* | *AA:NN*] | **permit** *community-number* } [**seq** *seq-value*] [**internet** | **local-as** | **no-advertise** | **no-export**]

no ip community-list standard *community-list-name*

Command Default

This option is disabled.

Parameters

community-list-name
Range is from 1 through 32 ASCII characters.

community-number
A community number. Range is from 1 through 4294967295.

AA **:** *NN*
Autonomous system number and network number, configured as 2-byte numbers separated by a colon.

seq
Sequence number. Range is from 1 through 65535.

internet
The Internet community.

no-export
Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGP neighbors.

local-as
Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.

no-advertise
Routes with this community cannot be advertised to any other BGP4 devices at all.

Modes

RBridge ID configuration mode

Usage Guidelines

A standard community list does not accept a regular expression.

Use the **no** form of this command to restore the default.

Examples

To create a standard community list:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip community-list standard seq 10 permit local-as
```

Related Commands

ip community-list extended, seq (IPv6 standard ACLs)

ip dhcp relay address

Configures the IP DHCP Relay on a Layer 3 interface.

Syntax

ip dhcp relay address *ip-addr* [**use-vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

use-vrf

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name

VRF name.

Modes

Interface configuration mode

Usage Guidelines

This command uses the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or a physical GigabitEthernet, TengigabitEthernet, or FortyGigabitEthernet interface

Enter the command while in interface configuration mode for a VE or physical interface where you want to configure the IP DHCP Relay. Configure up to four DHCP server IP addresses per interface. Use the **no** version of this command to remove the IP DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

Examples

To configure an IP DHCP Relay address on a VE interface::

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)interface ve 101
switch(config-Ve-101)# ip dhcp relay address 100.1.1.2
switch(config-Ve-101)# ip dhcp relay address 12.3.4.6
```

To configure an IP DHCP Relay address on an interface if the DHCP server is on a different VRF than the interface where the client connects:

```
switch# config
Entering configuration mode terminal
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# interface ve 103
switch(config-Ve-103)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

Related Commands

show ip dhcp relay address interface

ip directed-broadcast

Enables IP directed broadcasts on an interface. A directed broadcast is an IP broadcast to all devices within a single directly attached network or subnet.

Syntax

ip directed-broadcast

no ip directed-broadcast

Command Default

ip directed broadcast is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip directed-broadcast** to disable IP directed broadcasts on a specific interface.

Examples

To enable IP directed broadcasts on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip directed-broadcast
```

To disable IP directed broadcasts on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip directed-broadcast
```

Related Commands

interface, interface ve

ip dns

Sets the domain name service (DNS) parameters.

This command configures the DNS domain name and name-server IP address. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers

Syntax

ip dns { **domain-name** *domain_name* | **name-server** *ip_address_of_name_server* }

no ip dns { **domain-name** *domain_name* | **name-server** *ip_address_of_name_server* }

Parameters

domain-name *domain_name*
The domain name for the primary and secondary name servers.

name-server *ip_address_of_name_server*
The IP address of the primary and secondary name servers. IPv6 and IPv4 addresses are supported.

Modes

Global configuration mode

Usage Guidelines

You can enter only two name server IP addresses.

Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.

NOTE
If a domain name is not configured by means of the **domain-name** operand, DNS configuration will not work and a warning message will appear.

Enter **no ip dns domain-name** *domain_name* to disable IP directed broadcasts for a specific domain.

Enter **no ip dns name-server** *ip_address_of_name_server* to disable IP directed broadcasts for a specific name server.

Examples

To configure DNS:

```
switch(config)# ip dns domain-name  brocade.com
switch(config)# ip dns name-server  10.70.20.1
switch(config)# ip dns name-server  10.70.20.10
```

Related Commands

show running-config ip dns

ip echo-reply

Enables the generation of an Internet Control Message Protocol (ICMP) Echo Reply message.

Syntax

ip echo-reply

no ip echo-reply

Modes

Global configuration mode

Usage Guidelines

This is an interface-specific configuration. The configuration is persistent across a switch reload.

ip extcommunity-list

Sets a BGP extended community filter.

Syntax

ip extcommunity-list *number* { **deny** | **permit** [**rt** *value*] [**soo** *value*] }

ip extcommunity-list *number*

Command Default

No BGP extended community filter is set.

Parameters

number

Specifies an Extended Community list Instance number.

deny

Denies access for a matching condition.

permit

Permits access for a matching condition.

rt

Specifies the route target (RT) extended community.

value

Specifies the RT extended community value. This value can be entered in one of the following formats:

- autonomous-system-number : network-number
- ip-address : network-number

soo

Specifies the site of origin (SOO) extended community.

value

Specifies the SOO extended community value. This value can be entered in one of the following formats:

- autonomous-system-number : network-number
- ip-address : network-number

Modes

Rbridge-ID configuration mode

Usage Guidelines

Use the no form of this command to delete a BGP extended community filter.

Examples

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip extcommunity-list 1 permit rt 123:2
device(config-rbridge-id-122)# ip extcommunity-list 1 deny soo 124:1
```

History

Release version	Command history
5.0.0	This command was introduced.

ip http-server enable

Enables the HTTP server. Once enabled, the HTTP daemon starts without the need to reboot.

Syntax

ip http-server enable

no ip http-server enable

Command Default

The HTTP server is disabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **no ip http-server enable** command to disable the HTTP server. All active HTTP connections are closed, followed by a restart of the Apache server.

ip icmp rate-limit

Limits the rate at which Internet Control Message Protool (ICMP) messages are sent on an IPv4 network.

Syntax

ip icmp rate-limit *milliseconds*

no ip icmp rate-limit

Command Default

The default value is 1000 milliseconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The configuration is persistent across a switch reload. Once it is enabled, all outbound ICMP message types are rate limited.

ip igmp immediate-leave

Removes a group from the IGMP table immediately when receiving a Leave Group request.

This command treats the interface as if it had one multicast client, so receipt of a Leave Group request on the interface causes the group to be immediately removed from the multicast database.

Syntax

ip igmp immediate-leave

no ip igmp immediate-leave

Command Default

This command is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp immediate-leave** to restore the default setting.

ip igmp last-member-query-interval

Sets the last-member query interval for a VLAN.

Syntax

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

Command Default

1000 milliseconds

Parameters

milliseconds

Response time in milliseconds. Valid values range from 100 through 25500 milliseconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The last-member query interval is the time in seconds that the IGMP router waits to receive a response to a group-specific query message, including messages sent in response to a host-leave message.

Enter **no ip igmp last-member-query-interval** to remove the last-member query interval on a specific interface.

Examples

To set the last-member query interval to 1500 milliseconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# ip igmp last-member-query-interval 1500
```

ip igmp query-interval

Sets the query interval for a VLAN. The query interval is the amount of time between IGMP query messages sent by the switch.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

Command Default

125 seconds

Parameters

seconds

Response time in seconds. Valid values range from 1 through 18000 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp query-interval** to remove the query interval on a specific VLAN interface.

Examples

To set the query interval to 500 seconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# ip igmp query-interval 500
```

To remove the query interval from a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-Vlan-100)# no ip igmp query-interval
```

ip igmp query-max-response-time

Sets the maximum response time for IGMP queries for a VLAN.

Syntax

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Command Default

10 seconds

Parameters

seconds

Response time in seconds. Valid values range from 1 through 25 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, the switch (host) replies with a report, provided that no other host from the same group has responded yet.

Enter **no ip igmp query-max-response-time** to restore the default maximum response time for IGMP queries.

Examples

To set the maximum response time to 20 seconds on a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-vlan-100)# ip igmp query-max-response-time 20
```

To remove the maximum response time from a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(conf-vlan-100)# no ip igmp query-max-response-time
```

ip igmp snooping enable (global version)

Enables Internet Group Management Protocol (IGMP) snooping for all VLAN interfaces.

Syntax

ip igmp snooping enable

no ip igmp snooping enable

Command Default

IGMP snooping is globally disabled.

Modes

Global configuration mode

Usage Guidelines

This command enables IGMP snooping at the global level causing feature to be automatically enabled at all the already configured VLANs. In presence of this command, later if a VLAN is created, IGMP snooping will get enabled for that VLAN as well.

Enter **no ip igmp snooping enable** to return to the default setting.

Examples

To enable IGMP globally:

```
switch(config)# ip igmp snooping enable
```

Related Commands

ip igmp snooping enable, show ip igmp snooping

ip igmp snooping enable

Enables Internet Group Management Protocol (IGMP) snooping for a specific VLAN interface.

Syntax

ip igmp snooping enable

no ip igmp snooping enable

Command Default

When snooping is enabled globally, IGMP snooping is enabled on all VLAN interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Enter **no ip igmp snooping enable** to disable snooping for a specific VLAN interface.

Examples

To enable IGMP for a specific VLAN interface:

```
switch(config)# interface vlan 1
switch(config-Vlan-1)# ip igmp snooping enable
```

To disable IGMP for a specific VLAN interface:

```
switch(config)# interface vlan 1
switch(config-Vlan-1)# no ip igmp snooping enable
```

ip igmp snooping fast-leave

Enables Internet Group Management Protocol (IGMP) snooping fast-leave processing for a VLAN. This allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface

Syntax

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Command Default

This command is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp snooping fast-leave** to disable this function.

Examples

To enable snooping fast-leave for a specific VLAN interface:

```
switch(config)# interface vlan 1
switch(config-Vlan-1)# ip igmp snooping fast-leave
```

To disable snooping fast-leave for a specific VLAN interface:

```
switch(config)# interface vlan 1
switch(config-Vlan-1)# no ip igmp snooping fast-leave
```

ip igmp snooping mrouter

Configures a VLAN port member to be a multicast router interface. A multicast router interface faces toward a multicast router or other Internet Group Management Protocol (IGMP) querier.

Syntax

ip igmp snooping mrouter { *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* }

no ip igmp snooping mrouter { *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* }

Parameters

interface

Specifies an interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the interface is a port-channel. Valid values range from 1 through 6144.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp snooping mrouter** to remove the configured mrouter.

This command is mutually exclusive of **ip igmp snooping querier enable**.

Examples

To configure a VLAN port member to be a multicast router interface.

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping mrouter interface tengigabitethernet 101/0/1
```

ip igmp snooping mrouter-timeout

Configures the mrouter timeout value for Internet Group Management Protocol (IGMP) snooping on a VLAN. The timeout range determines when multicast router ports are automatically learned on a specific VLAN interface.

Syntax

ip igmp snooping mrouter-timeout *seconds*

no ip igmp snooping mrouter-timeout

Command Default

300 seconds

Parameters

seconds

Timeout time in seconds. Valid range is from 1 through 60000 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp snooping mrouter-timeout** to restore the default mrouter value of 300 seconds on the VLAN interface.

Examples

To configure the mrouter timeout value to 600 seconds on a VLAN interface:

```
switch(config)# interface vlan 100

switch(config-Vlan-100)# ip igmp snooping mrouter-timeout 600
```

ip igmp snooping querier enable

Activates or deactivates the Internet Group Management Protocol (IGMP) snooping querier on a VLAN.

Syntax

ip igmp snooping querier enable

no ip igmp snooping querier enable

Command Default

IGMP snooping querier is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip igmp snooping querier enable** to disable the IGMP snooping querier.

This command is mutually exclusive of **ip igmp snooping mrouter interface** .

Examples

To enable the IGMP snooping querier feature for the VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping querier enable
```

ip igmp snooping restrict-unknown-multicast

Activates or deactivates the Internet Group Management Protocol (IGMP) snooping hello-based mrouter detection functionality.

Syntax

ip igmp snooping restrict-unknown-multicast

no ip igmp snooping restrict-unknown-multicast

Command Default

IGMP snooping restrict-unknown-multicast is enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

The PIM hello-based multicast router presence detection feature scans the network traffic for incoming PIM hellos. When a PIM hello is detected, that port is marked for the presence of a multicast router and the information is saved. This prevents unnecessary flooding if the PIM designated router (DR) goes offline, as IGMP reports are forwarded to the multicast routers and not only the snooping enabled router.

Enter **no ip igmp snooping restrict-unknown-multicast** to disable the hello-based mrouter detection functionality.

Examples

To enable the IGMP snooping hello-based mrouter detection functionality feature for the VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp snooping restrict-unknown-multicast
```

ip igmp static-group

Configures the static group membership entries for a specific interface.

Syntax

ip igmp static-group *A.B.C.D*

no ip igmp static-group *A.B.C.D*

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

Modes

Interface subtype configuration mode

Usage Guidelines

This command to creates IGMP static group membership to test multicast forwarding without a receiver host.

When you enable IGMP static group membership, data is forwarded to an interface without receiving membership reports from host members. Using **ip igmp static-group** , packets to the group are fast-switched out of a specific interface. Static group membership entries are automatically added to the IGMP cache and PIMmcache table. Enter **no ip igmp static-group** *A.B.C.D* to restore the default setting for the specified group address.

Examples

To create a static port-channel group for a specific VLAN interface:

```
switch(config)# interface vlan 100
switch(config-Vlan-100)# ip igmp static-group 225.1.1.1 interface port-channel 60
```

To reset a static group on a specific VLAN interface to the default settings:

```
switch(config)# interface vlan 100
 switch(config-Vlan-100)# no ip igmp static-group 225.1.1.1
```

ip import routes (IPv4 VRF address-family configuration mode)

Leaks IPv4 routes from one VRF to the VRF you are configuring, based on match criteria defined in route-map.

Syntax

ip import routes *VRF_name* **map** *rmap_name*

no ip import routes

Parameters

VRF_name
Specifies the VRF instance from which to leak routes to the VRF you are configuring.

rmap_name
Specifies the map name to use for route-leaking match criteria.

Modes

IPv4 VRF address-family configuration mode

Usage Guidelines

Use the **no** form of the command to remove routes from being leaked to the VRF you are configuring.

Examples

To leak IPv4 routes from a VRF named "red" to the VRF named "orange," based on match criteria from a route map named "import-map," with an example RBridge ID of 10:

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# vrf orange
switch(config-vrf-orange)# address-family ipv4 unicast
switch(config-ipv4-unicast)# ip import routes red route-map import-map
```

History

Release version	Command history
5.0.0	This command was introduced.

ip import routes (RBridge ID configuration mode)

Leaks IPv4 routes from the specified VRF to the default VRF, based on match criteria defined in route-map.

Syntax

ip import routes *VRF_name* **map** *rmap_name*

no ip import routes

Parameters

VRF_name
Specifies the VRF instance from which to leak routes to the default VRF.

rmap_name
Specifies the map name to use for route-leaking match criteria.

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no** form of the command to remove routes from being leaked to the default VRF.

Examples

To leak IPv4 routes from a VRF named "red" to the default VRF, based on match criteria from a route map named "import-map" :

```
switch# configure
switch(config)# rbridge-id 54
switch(config-rbridge-id-54)# ip import routes red map import-map
```

History

Release version	Command history
5.0.0	This command was introduced.

ip interface

Sets the IP address of the VXLAN overlay gateway instance.

Syntax

ip interface { **ve** *veid* **vrrp-extended-group** *group-ID* | **loopback** *ifid* }

no ip interface

Parameters

ve *veid*

Specifies the ID of the virtual Ethernet (VE) interface (which must already be configured) through which you are configuring the IP address of the VXLAN gateway.

vrrp-extended-group *group-ID*

Specifies the virtual router group (which must already be configured) through which you are configuring the IP address of the VXLAN gateway.

loopback *ifid*

Specifies an IPv4 loopback interface ID (IPv6 addresses are ignored). The range is from 1 through 255.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

The VXLAN overlay gateway IP address is also the source IP address for all the tunnels associated with the gateway. The command accepts the VE interface ID and VRPP-E group ID, then sets the overlay gateway IP address to be identical to the already configured Virtual Redundancy Router Protocol-Extended (VRRP-E) virtual IP address.

Ensure that the VXLAN gateway is in the inactive state when you issue this command. Use the **no activate** command in VXLAN overlay gateway configuration mode to deactivate the gateway.

If a specified loopback ID does not exist, or if the loopback interface is not fully configured, the **activate** command is rejected.

If you have already added RBridge attachments to the VXLAN gateway overlay, the VE and VRPP-E group IDs must exist for the attached RBridge IDs.

Changing the VE interface ID or VRRP-E group ID requires an update of all tunnel source addresses.

Use the **no** form of this command to delete the IP address configuration for this gateway.

Some commands cannot be used if they would affect an active VXLAN gateway address configuration. For example, consider the following configuration:

```
switch# configure
switch(config)# overlay-gateway xx
switch(config-overlay-gw-xx)# attach rbridge-id add 1
switch(config-overlay-gw-xx)# ip interface ve 1000 vrrp-extended-group 100
switch(config-overlay-gw-xx)# activate
```

Examples of operations that would not be allowed based on this configuration are:

- Deleting VLAN 1000 (because this implicitly deletes VE 1000)
- Deleting VE 1000 on Rbridge 1
- Deleting VRRP-E group 100 for VE 1000 on Rbridge 1
- Changing virtual IP configuration for VE 1000, VRRPE group 100 on Rbridge 1
- Changing VRF on VE 1000 on Rbridge 1

Examples

To set the IP address of a VXLAN gateway overlay named "gateway1" (using the already configured Ve interface ID 10 and the vrrp-extended group ID 25):

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# ip interface ve 10 vrrp-extended-group 25
```

ip mtu

Sets the MTU on a speciffied interface.

Syntax

ip mtu *size*

no ip mtu

Command Default

MTU size is 1500 bytes.

Parameters

size

Specifies the size of the maximum transmission unit (MTU) of an interface.

Modes

Interface subtype configuration mode

Usage Guidelines

The entire fabric acts like a single switch. Therefore, MTU is applicable only on edge ports and not on an ISL.

The allowed MTU size is from 576 to 9018 bytes.

Enter **no ip mtu** to reset the MTU size to the default.

Examples

To set the MTU size to 2000 bytes on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip mtu 2000
```

Related Commands

interface

ip multicast-boundary

Configures a multicast boundary on an interface.

Syntax

ip multicast-boundary

no ip multicast-boundary

Command Default

No multicast boundaries are defined on an interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Since there is no support for a prefix-list, this command applies the boundary for the entire multicast range on the interface.

Enter **no ip multicast-boundary** to disable this feature.

ip ospf active

Sets a specific OSPF interface to active.

Syntax

ip ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

Examples

To set a specific OSPF virtual Ethernet (VE) interface to active:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# int ve 100
sw0(config-Ve-100)# ip ospf active
```

Related Commands

ip ospf passive

ip ospf area

Enables OSPF on an interface.

Syntax

ip ospf area *area-id*

no ip ospf area

Command Default

OSPF is disabled.

Parameters

area-id

Area address in dotted decimal or decimal format.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to enable an OSPF area on the interface to which you are connected.

Enter **no ip ospf area** to disable OSPF on this interface.

Examples

To enable a configured OSPF area named 0 on a specific OSPF 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf area 0
```

To enable a configured OSPF area named 0 on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 12
switch(config-ve-12)# ip ospf area 0
```

ip ospf auth-change-wait-time

Configures authentication-change hold time.

Syntax

ip ospf auth-change-wait-time *wait-time*

no ip ospf auth-change-wait-time

Command Default

Wait time is 300 seconds

Parameters

wait-time

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the authentication change hold time for the interface to which you are connected.

OSPF provides graceful authentication change for the following types of authentication changes:

Changing authentication methods from one of the following to another of the following:

- Simple text password
- MD5 authentication
- No authentication

Configuring a new simple text password or MD5 authentication key.

Changing an existing simple text password or MD5 authentication key

Enter **no ip ospf auth-change-wait-time** to reset the wait time to the default of 300 seconds.

Examples

To set the wait time to 600 seconds on a specific OSPF 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf auth-change-wait-time 600
```

To set the wait time to 400 seconds on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 12
switch(config-ve-12)# ip ospf auth-change-wait-time 400
```

ip ospf authentication-key

Configures simple password-based authentication for OSPF.

Syntax

ip ospf authentication-key { **0** *password* | **2** *password* | **255** *password* | *password* }

no ip ospf authentication-key

Command Default

No authentication.

Parameters

0 *password*

No encryption. OSPF processes *password* as a plain text password and shows the unencrypted password in the **show running** command output as follows: `key 0 passwd`

2 *password*

Expects the user to provide the encrypted password, preceded by a dollar sign ($) sign, and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

255 *password*

Expects the user to provide the encrypted password, and **255** internally maps to **2** . OSPF shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

password

OSPF processes *password* as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to sets or reset simple password-based authentication on the OSPF interface to which you are connected.Enter **no ip ospf authentication-key** to disable OSPF authentication.

Examples

The following command sets authentication only on the OSPF 10-gigabit Ethernet interface 190/0/49. To enter a plain text password called brocade that OSPF will encrypt as if encryption key 2 was specified:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf authentication-key brocade
```

The following example sets authentication on the OSPF virtual Ethernet (VE) interface 12, with a plain text password called brocade that OSPF will encrypt as if encryption key 2 was specified:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 12
switch(config-ve-12)# ip ospf authentication-key brocade
```

ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost *value*

no ip ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPF cost on the interface. If the cost is not configured with this command, OSPF calculates the value from the reference and interface bandwidths.

Enter **no ip ospf cost** to disable this configuration.

Examples

To set the cost to 600 on a specific OSPF 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf cost 600
```

To set the cost to 520 on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 12
switch(config-ve-12)# ip ospf cost 520
```

ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Syntax

ip ospf database-filter { **all-external** { **allow-default-and-type-4** | **allow-default-out** | **out** } | **all-out** | **all-summary-external** { **allow-default-and-type-4** | **allow-default-out** | **out** } }

no ip ospf database-filter all-external

no ip ospf database-filter all-out

no ip ospf database-filter all-summary-external

Command Default

All filters are disabled.

Parameters

all-external
Blocks all external LSAs.

allow-default-and-type-4
Allows default-route LSAs and Type 4 LSAs, but block all other LSAs.

allow-default-out
Allows default-route LSAs, but block all other LSAs.

out
Filters outgoing LSAs.

all-out
Blocks all LSAs.

all-summary-external
Blocks all summary (Type 3) and external (type 5) LSAs.

Modes

Interface subtype configuration mode

Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area. When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
- To use a passive router for debugging only.

Enter **no ip ospf database-filter** followed by the appropriate operands to disable this configuration.

NOTE
You cannot block LSAs on virtual links.

Examples

To apply a filter to block flooding of all LSAs on a specific OSPF 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# ip ospf database-filter all-out
```

To apply a filter to block flooding of all LSAs on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf database-filter all-out
```

ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ip ospf dead-interval *interval*

no ip ospf dead-interval

Command Default

The default value is 40 seconds.

Parameters

interval

Dead interval in seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

f you change the dead interval, the hello interval is changed to be one fourth the new dead interval, unless the hello interval is also explicitly configured by using the **ip ospf hello-interval** command. Also, **running-config** displays only explicitly configured values of the hello interval, which means that a value that got automatically changed as the result of a dead-interval change would not be displayed.

Enter **no ip ospf dead-interval** to use the default value.

Examples

To set the dead interval to 80 on a specific OSPF 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# ip ospf dead-interval 80
```

To set the dead interval to 70 on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf dead-interval 70
```

ip ospf hello-interval

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to neighbor routers.

Syntax

ip ospf hello-interval *interval*

no ospf hello-interval

Command Default

The default value is 10 seconds.

Parameters

interval

Hello interval in seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is changed to be four times the new hello interval, unless the dead interval is also explicitly configured using the **ip ospf dead-interval** command. Also, **running-config** displays only explicitly configured values of the dead interval, which means that a value that got automatically changed as the result of a hello-interval change would not be displayed.

Enter **no ospf hello-interval** to use the default value.

Examples

To set the hello interval to 200 on a specific OSPF 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# ip ospf hello-interval 200
```

To set the hello interval to 180 on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf hello-interval 180
```

ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

Syntax

ip ospf md5-authentication { **key-activation-wait-time** *wait-time* | **key-id** *id MD5_key* { **0** | **2** | **255** } *ospf_password* }

no ip ospf md5-authentication key-id

Command Default

No authentication.

Parameters

key-activation-wait-time

Sets the time that OSPF waits before activating a new key.

wait-time

Time OSPF waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds. The default value is 300 seconds.

key-id

Sets MD5 key and OSPF password.

id MD5_key

The *num* is a number between 1 and 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the *key* is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

0 *password*

No encryption. OSPF processes **password** as a plain text password and shows the unencrypted password in the **show running** command output as follows: `key 0 passwd`

2 *password*

Expects the user to provide the encrypted password, preceded by a dollar sign ($), and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

255 *password*

Expects the user to provide the encrypted password, and **255** internally maps to **2**. OSPF shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

ospf_password

OSPF processes *password* as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the **show running** command output as follows: `key 2 $ci1pVT0=`

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

Enter **no ip ospf md5-authentication key-id** to disable this configuration.

Examples

The following command sets authentication only on the OSPF 40-gigabit Ethernet interface 100/0/1. To enter an MD5 ID/key of **255 key** and a plain text OSPF password called brocade that OSPF will encrypt as if encryption key **2** was specified:

```
switch(config)# interface fortygigabitethernet 100/0/1
switch(conf-if-fo-100/0/1)# ip ospf md5 key-id 255 key brocade
```

The following command sets authentication only on the OSPF virtual Ethernet (VE) interface 24. To enter an MD5 id/key of **255 key** and a plain text OSPF password called brocade that OSPF will encrypt as if encryption key **2** was specified:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf md5 key-id 255 key brocade
```

ip ospf mtu-ignore

Enables or disables MTU-match checking.In default operation, the IP MTU on both sides of an OSPF link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Command Default

Enabled

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip ospf mtu-ignore** to disable MTU-match checking on a specific interface.

Examples

To disable MTU-match checking on a specific OSPF 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 101/0/10
switch(conf-if-fo-101/0/10)# no ip ospf mtu-ignore
```

To disable MTU-match checking on a specific OSPF virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# no ip ospf mtu-ignore
```

ip ospf network

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

Syntax

ip ospf network { **broadcast** | **point-to-point** }

no ip ospf network

Parameters

broadcast
Network type is broadcast, such as Ethernet.

point-to-point
Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip ospf network** to remove the network-type configuration.

NOTE
The network type non-broadcast is not supported at this time.

Examples

To configure an OSPF point-to-point link on the OSPF 10-gigabit Ethernet interface whose rbridge-ID/slot/port format is 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf network point-to-point
```

To configure an OSPF broadcast link on the OSPF virtual Ethernet (VE) interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf network broadcast
```

ip ospf passive

Configures an OSPF interface as passive.

Syntax

ip ospf passive

no ip ospf passive

Command Default

All OSPF interfaces are active.

Modes

Interface subtype configuration mode

Usage Guidelines

Passive interfaces accept and process all OSPF protocol traffic, but they do not send any traffic.

You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

Enter **no ip ospf passive** to set an interface back to active.

Examples

To set a specific OSPF 10-gigabit Ethernet interface to passive state:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf passive
```

To set a specific OSPF virtual Ethernet (VE) interface to passive state:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf passive
```

Related Commands

ip ospf active

ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority *value*

no ip ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set priority for DR election and backup-router election on the interface you are connected to. The OSPF router assigned the highest priority becomes the designated router, and the OSPF router with the second-highest priority becomes the backup router.

Enter **no ip ospf priority** to use the default value.

Examples

To set a priority of 10 for the OSPF router that is connected to an OSPF 10-gigabit Ethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf priority 10
```

To set a priority of 10 for the OSPF router that is connected to an OSPF virtual Ethernet (VE) interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf priority 10
```

ip ospf retransmit-interval

Configures retransmit interval. The interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for this interface.

Syntax

ip ospf retransmit-interval *rtx-int*

no ip ospf retransmit-interval

Command Default

5 seconds.

Parameters

rtx-int

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip ospf retransmit-interval** to reset the retransmit interval to its default.

Examples

To set the retransmit interval to 10 for all OSPF routers on the OS-gigabit Ethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf retransmit 10
```

To set the retransmit interval to 50 for all OSPF routers on the OSPF virtual Ethernet (VE) interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf retransmit 50
```

ip ospf transmit-delay

Configures the transmit delay for link-update packets, which is the estimated time required for OSPF to send link-state update packets on the interface to which you are connected.

Syntax

ip ospf transmit-delay *tx-delay*

no ip ospf transmit-delay

Command Default

1 second.

Parameters

tx-delay

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip ospf transmit-delay** to use the default value.

Examples

To set a transmit delay of 10 seconds for routers on the OSPF 10-gigabit Ethernet interface 190/0/49:

```
switch(config)# interface tengigabitethernet 190/0/49
switch(conf-if-te-190/0/49)# ip ospf transmit-delay 10
```

To set a transmit delay of 30 seconds for routers on the OSPF virtual Ethernet (VE) interface 24:

```
switch(config)# rbridge-id 178
switch(config-rbridge-id-178)# interface ve 24
switch(config-ve-24)# ip ospf transmit-delay 30
```

ip pim dr-priority

Configures the designated router (DR) priority of a protocol Independent Multicast (PIM) enabled interface.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority

Command Default

DR priority value is 1.

Parameters

priority-value

The DR priority value. Valid values range from 0 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip pim dr-priority** to disable this feature.

Examples

Setting the priority to 100.

```
switch(conf-if-ext-0/15)# ip pim dr-priority 100
```

Related Commands

router pim

ip pim-sparse

Enables or disables Protocol Independent Multicast Sparse Mode on a physical or a VE interface.

Syntax

ip pim-sparse

no ip pim-sparse

Command Default

Protocol Independent Multicast (PIM) is not enabled on an interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip pim-sparse** to disable this feature.

Examples

Enabling sparse PIM on an interface

```
switch(conf-if-ext-0/15)# ip pim-sparse
```

Related Commands

router pim

ip policy route-map

Enables policy-based routing (PBR) on any Layer 3 interface after ACLs and route map entries are configured.

Syntax

ip policy route-map *map-tag*

no ip policy route-map *map-tag*

Parameters

map-tag

The name of the route-map when it was created.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no ip policy route-map** to disable this feature.

Related Commands

show route-map, show route-map interface

ip prefix-list

Configures the IP prefix-list instance.

Syntax

ip prefix-list *nameinstance* [**permit** | **deny**] *A.B.C.D/MLEN* **ge** *value* **le** *value*

no ip prefix-list *nameinstance* [**permit** | **deny**] *A.B.C.D/MLEN* **ge** *value* **le** *value*

Parameters

name

instance

permit

deny

A.B.C.D/MLEN

ge *value*

le *value*

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no ip prefix-list** to disable this feature.

DANGER

Cleanup item: This command has no parameter descriptions

ip proxy-arp

Enables proxy ARP on an interface.

Syntax

ip proxy-arp

no ip proxy-arp

Command Default

Proxy ARP is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Proxy ARP allows a Brocade device to answer ARP requests from devices on one network on behalf of devices in another network. Because ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Therefore, ARP requests do not cross routers.

Enter **no ip proxy-arp** to disable proxy ARP on a specific interface.

Examples

To enable proxy ARP on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ip proxy-arp
```

To disable proxy ARP on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no ip proxy-arp
```

Related Commands

interface, interface ve

ip route

Adds a static route to the IP routing tables.

Syntax

ip route *A.B.C.D/L A.B.C.D* [*metric*] [**distance** *distance*] [**tag** *tag*]

ip route *A.B.C.D/L* { *<N>***gigabitethernet** *slot/port* **ve** *vlan_id* } [*metric*] [**distance** *distance*] [**tag** *tag*]

ip route *A.B.C.D/L* **null** *slot/port* [*metric*] [**distance** *distance*] [**tag** *tag*]

no ip route *A.B.C.D/L A.B.C.D*

no ip route *A.B.C.D/L* { *<N>***gigabitethernet** *slot/port* | **ve** *vlan_id* }

no ip route *A.B.C.D/L* **null** *rbridge-id/slot/port*

Command Default

Refer to the Parameters descriptions for specific defaults.

Parameters

A.B.C.D/L

Specifies the destination IPv4 address and mask.

A.B.C.D

Specifies the IPv4 address of the next hop.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies the VLAN number. (Refer to the Usage Guidelines.)

null *slot/port*

Drops packets with this destination.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

metric

Cost metric of the route. Valid values range from 1through 16. The default is 1.

distance *distance*

Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, a Brocade device prefers lower administrative distances over higher ones. Valid values range from 1 through 255. The default is 1.

tag *tag*

Tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295.

Modes

RBridge ID configuration mode

Usage Guidelines

Enter **no ip route** followed by the route identifier to remove a static route.

Examples

To configure a static route to 10.95.7.0, using 10.95.6.157 as the next-hop gateway:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route 10.95.7.0/24 10.95.6.157
```

ip route next-hop-vrf

Enables the leaking of static routes from one VRF instance to another.

Syntax

ip route *ip_addr/mask* **next-hop-vrf vrf** *VRF_name next_hop_ip_addr*

no route *ip_addr/mask* **next-hop-vrf vrf** *VRF_name next_hop_ip_addr*

Command Default

Disabled

Parameters

ip_addr/mask
IPv4 address in dotted-decimal notation with a CIDR notation mask.

vrf *VRF_name*
Specifies the name of the target VRF instance to which route leaking is enabled.

ip_addr
Next-hop IP address in the target VRF instance.

Modes

RBridge ID configuration mode

VRF address-family IPv4 configuration mode

Usage Guidelines

Enter **no ip route** *ip_addr mask* **next-hop-vrf** to disable the leaking of static routes.

Examples

To enable static route leaking from the default VRF to VRF "brown":

```
switch# config
switch (config)# rbridge-id 2
switch (config-rbridge-id-2)# ip route 1.1.1.0/24 next-hop-vrf brown 10.1.1.10
```

This example shows the static route leaking enabled from the default VRF to VRF "brown":

```
switch# show running rbridge

rbridge-id 2
ip route 0.0.0.0/0 10.24.64.1
ip route 1.1.1.0/24 next-hop-vrf brown 10.1.1.10
```

ip router-id

Configures router ID.

Syntax

ip router-id *A.B.C.D*

no ip router-id *A.B.C.D*

Parameters

A.B.C.D

Specifies the IPv4 address that you want as the router ID.

Modes

RBridge ID configuration mode

Usage Guidelines

The router ID is a 32-bit number that uniquely identifies the device. By default, the router ID is the numerically lowest IP interface configured on the device, but you can explicitly set the router ID to any valid IP address that is not in use on another device in the network.

Enter **no ip router-id** *A.B.C.D* to remove the router ID and use the default router ID.

Examples

To specify a router ID of 192.158.1.2:

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip router-id 192.158.1.2
```

ip unreachable

Prohibits routers from forwarding an Internet Control Message Protocol (ICMP) Destination Unreachable Code 3 (port unreachable) message on a point-to-point link back onto the ingress port.

Syntax

ip unreachable

no ip unreachable

Command Default

This command is enabled by default.

Modes

Global configuration mode

Usage Guidelines

By default, ICMP Destination Unreachable Code 3 messages are sent for a discarded IP packet.

Use the **no ip unreachable** command to disable the sending of these messages.

This is an interface-specific configuration The configuration is persistent across a switch reload.

Related Commands

ipv6 unreachable

ipv6 access-group

Applies rules specified in an IPv6 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ipv6 access-group *ACLname* { **in** | **out** }

no ipv6 access-group *ACLname* { **in** | **out** }

Parameters

ACLname
Specifies the name of the standard or extended IP access list.

in | **out**
Specifies the binding direction (ingress or egress).

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv6 ACL to one of the following interface types:

- User interfaces
  - Physical interfaces (<N>-gigabit Ethernet)
  - Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- All supported management interfaces
- Overlay gateways

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL
- One egress MAC ACL
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL
- One egress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of three ACLs to an overlay gateway, as follows:

- One ingress MAC ACL
- One ingress IPv4 ACL

- One ingress IPv6 ACL

  NOTE
  You can apply an ACL to multiple interfaces. And you can apply an extended ACL twice—ingress and egress—to a given user interface.

To remove an IPv6 ACL from an interface, enter the **no ipv6 access-group** *ACLname*

Examples

The following example applies an ingress IPv6 ACL named ip6_acl_7 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# ipv6 access-group ip6_acl_7 in
```

The following example removes an ingress IPv6 ACL named ip6_acl_7 from a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no ipv6 access-group ip6_acl_7 in
```

Related Commands

interface, ipv6 access-list, show access-list

ipv6 access-list

Creates a standard or extended IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ipv6 access-list { **standard** | **extended** } *ACLname*

no ipv6 access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:

standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

On any given switch, an ACL name must be unique among all ACL types (MAC/IPv4/IPv6; standard or extended).

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after if is applied to an interface, using the **access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv6 standard ACL:

```
switch# configure
switch(config)# ipv6 access-list standard stdV6ACL1
```

The following example creates an IPv6 extended ACL:

```
switch# configure
switch(config)# ipv6 access-list extended ipv6_acl_1
```

The following example creates rules on an IPv6 standard ACL:

```
switch# configure
switch(config)# ipv6 access-list standard stdV6ACL1
switch(config-ipv6-std)# seq 10 permit 2001:db8:85a3:0:0:8a2e:370:7334
switch(config-ipv6-std)# seq 11 deny any
```

The following example deletes an IPv6 ACL:

```
switch# configure
switch(config)# no ipv6 access-list standard stdV6ACL1
```

ipv6 address

Configures a primary or secondary global or unique local IPv6 unicast address, including a manually configured interface ID.

Syntax

ipv6 address *ipv6-prefix/prefix-length* [**secondary**]

no ipv6 address *ipv6-prefix/prefix-length* [**secondary**]

Command Default

If the **secondary** keyword is not used, the address is a primary address.

Parameters

ipv6-prefix
IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

secondary
Specifies that the address is a secondary address. A maximum of 256 secondary addresses can be configured.

Modes

Interface subtype configuration mode

Usage Guidelines

A secondary address cannot be configured on an interface unless the primary address is configured first.

Use the **no** form of this command to remove the configuration.

The primary address cannot be deleted on an interface unless the secondary addresses are deleted first.

This command is not supported on loopback or management interfaces.

Examples

To configure a global prefix and the interface ID on an Ethernet interface:

```
switch(config)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

To configure the above as a secondary address:

```
switch(config)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64 secondary
```

ipv6 address anycast

Configures an anycast address for a set of interfaces that belong to different nodes.

Syntax

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address *ipv6-prefix/prefix-length* **anycast**

Parameters

ipv6-prefix
IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

Modes

Interface subtype configuration mode

Usage Guidelines

Sending a packet to an anycast address results in the delivery of the packet to the closest interface that has an anycast address. An anycast address looks similar to a unicast address, because it is allocated from the unicast address space. If you assign an IPv6 unicast address to multiple interfaces, it is an anycast address. On the device, you configure an interface assigned an anycast address to recognize the address as an anycast address

If you assign an IPv6 unicast address to multiple interfaces, it is an anycast address. On the device, you configure an interface assigned an anycast address to recognize the address as an anycast address.

Use the **no** form of this command to remove the configuration.

NOTE
IPv6 anycast addresses are described in detail in RFC 1884. See RFC 2461 for a description of how the Neighbor Discovery mechanism handles anycast addresses.

Examples

To configure an anycast address on an Ethernet interface:

```
switch(config)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64 anycast
```

ipv6 address eui-64

Configures a global or unique local IPv6 unicast address with an automatically computed EUI-64 interface ID.

Syntax

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address *ipv6-prefix/prefix-length* **eui-64**

Parameters

ipv6-prefix
IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

eui-64
Configures the global or unique local unicast address with a 64-bit Extended Unique Identifier, using the MAC address of the interface to construct the interface ID automatically.

Modes

Interface subtype configuration mode

Examples

To configure a global prefix and an automatically computed EUI-64 interface ID on a TenGigabitEthernet interface:

```
switch(config)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 address 2001:db8:12d:1300::/64 eui-64
```

ipv6 address link-local

Configures an explicit link-local address on an interface.

Syntax

ipv6 address *ipv6-address* **link-local**

no address *ipv6-address* **link-local**

Parameters

ipv6-address

Explicit IPv6 address for the interface. Format can be xxxx.xxxx or xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.

Modes

Interface subtype configuration mode

Usage Guidelines

By default,when IPv6 is enabled, link-local addresses are computed automatically.

When configuring VLANs that share a common tagged interface with a virtual Ethernet (VE) interface, it is recommended that you override the automatically computed link-local address with a manually configured unique address for the interface. If the interface uses the automatically computed address, which in the case of VE interfaces is derived from a global MAC address, all VE interfaces will have the same MAC address.

Examples

To configure a unique link-local address on an Ethernet interface:

```
switch(config)# int te 3/0/1
switch(config-if-te-3/0/1)# ipv6 address fe80::240:d0ff:fe48:4672 link-local
```

Related Commands

ipv6 address use-link-local-only

ipv6 address use-link-local-only

Enables IPv6 on an interface and configures an automatically computed link-local address.

Syntax

ipv6 address use-link-local-only

no ipv6 address use-link-local-only

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to disable IPv6 on an interface and consequently the automatic computing of a link-local address.

Examples

To enable IPv6 on an interface and configure an automatically computed link-local address:

```
switch(config)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 address use-link-local-only
```

Related Commands

ipv6 address link-local

ipv6 dhcp relay address

Configures the IPv6 DHCP Relay on a Layer 3 interface.

Syntax

ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

no ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of the DHCP server where the DHCP client requests are to be forwarded.

interface
This parameter specifies the outgoing interface, used when the relay address is a link-local or multicast address

interface-type
The type of interface, such as gigabitEthernet, TengigabitEthernet, FortygigabitEthernet, HundredgigabitEthernet, or Ve interface.

interface-name
The interface number or VLAN ID.

use-vrf
Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name
VRF name.

Modes

Interface configuration mode

Usage Guidelines

This command uses the IPv6 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or a physical GigabitEthernet, TengigabitEthernet, or FortyGigabitEthernet interface. You can configure up to 16 relay destination addresses on an interface.

Enter the command while in interface configuration mode for a VE or physical interface where you want to configure the IPv6 DHCP Relay. Configure up to four DHCP server IP addresses per interface. Use the **no** version of this command to remove the IPv6 DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

If the relay address is a link local address or a multicast address, an outgoing interface must be configured for IPv6 relay to function. In instances where the server address is relayed to a different VRF compared to a client connected interface VRF, in addition to the relay address, you must also specify the user-vrf, otherwise IPv6 relay may not function correctly. IPv6 route leaking is also required for IPv6 reachability.

The **no** form of the command deletes the ipv6 dhcp relay from an L3 interface.

Examples

To configure an IPv6 DHCP Relay address on a TenGigabitEthernet interface in standalone mode:

```
sw0(config)# interface TenGiga 2/3/1
sw0(conf-if-te-2/3/1)# ipv6 dhcp relay address 2001::1122:AABB:CCDD:3344
```

To configure an IPv6 DHCP Relay address on a VE interface in VCS mode:

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)interface ve 101
switch(config-Ve-101)# ipv6 dhcp relay address fe80::224:38ff:febb:e3c0 interface ve 201
```

To configure an IPv6 DHCP Relay address on an interface if the DHCP server is on a different VRF than the interface where the client connects:

```
switch# config
Entering configuration mode terminal
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# interface ve 103
switch(config-Ve-103)# ipv6 dhcp relay address fe80::224:38ff:febb:e3c0 use-vrf blue
```

NOTE

For the relay configurations to be successful, you must specify an outgoing interface for any link local IPv6 relay addresses.

History

Release version	Command history
5.0.1	This command was introduced.

ipv6 echo-reply

Enables the generation of an Internet Control Message Protocol version 6 (ICMPv6) Echo Reply message.

Syntax

ipv6 echo-reply

no ipv6 echo-reply

Modes

Global configuration mode

Usage Guidelines

This is an interface-specific configuration. The configuration is persistent across a switch reload.

ipv6 icmp rate-limit

Limits the rate at which Internet Control Message Protocol (ICMP) messages are sent on an IPv6 network.

Syntax

ipv6 icmp rate-limit *milliseconds*

no ipv6 icmp rate-limit

Command Default

The default value is 1000 milliseconds.

Parameters

milliseconds

Number of milliseconds between packets. The range is from 1 through 4294967295.

Modes

Interface subtype configuration mode

Usage Guidelines

The configuration is persistent across switch reload. Once it is enabled, all outbound ICMP message types are rate limited.

Examples

Typical command example.

```
switch(conf-if-te-12/2/1)# ipv6 icmp rate-limit 3000
```

Related Commands

ip icmp rate-limit

ipv6 import routes (IPv6 VRF address-family configuration mode)

Leaks IPv6 routes from one VRF to the VRF you are configuring, based on match criteria defined in route-map.

Syntax

ipv6 import routes *VRF_name* **map** *rmap_name*

no ipv6 import routes

Parameters

VRF_name
Specifies the VRF instance from which to leak routes to the VRF you are configuring.

rmap_name
Specifies the map name to use for route-leaking match criteria.

Modes

IPv6 VRF address-family configuration mode

Usage Guidelines

Use the **no** form of the command to remove routes from being leaked to the VRF you are configuring.

Examples

To leak IPv6 routes from a VRF named "red" to the VRF named "orange," based on match criteria from a route map named "import-map," with an example RBridge ID of 10:

```
switch# configure
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# vrf orange
switch(config-vrf-orange)# address-family ipv6 unicast
switch(config-ipv6-unicast)# ipv6 import routes red route-map import-map
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 import routes(RBridge ID configuration mode)

Leaks IPv6 routes from the specified VRF to the default VRF, based on match criteria defined in route-map.

Syntax

ipv6 import routes *VRF_name* **map** *rmap_name*

no ipv6 import routes

Parameters

VRF_name
Specifies the VRF instance from which to leak routes to the default VRF.

rmap_name
Specifies the map name to use for route-leaking match criteria.

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no** form of the command to remove routes from being leaked to the default VRF.

Examples

To leak IPv6 routes from a VRF named **red** to the default VRF, based on match criteria from a route map named **import-map**:

```
switch# configure
switch(config)# rbridge-id 54
switch(config-rbridge-id-54)# ipv6 import routes red map import-map
```

History

Release version	Command history
	This command was introduced.

ipv6 mld last-member-query-count

Configures the IPv6 MLDv1 snooping last-member query count on a specific VLAN interface.

Syntax

ipv6 mld last-member-query-count *value*

no ipv6 mld last-member-query-count

Parameters

value

The range is from 1 through 10. The default is 2.

Modes

Interface subtype configuration mode

Usage Guidelines

The last-member query count is the number of times, separated by the last-member query-response interval, that an MLD query is sent in response to a host leave message from the last known active host on the subnet.

Use the **no** form of this command to restore the default.

Examples

To change the IPv6 MLDv1 snooping last-member query count from the default on a VLAN interface:

```
switch(config)# int vlan 2000
switch(config-Vlan-2000)# ipv6 mld last-member-query-count 3
```

Related Commands

ipv6 mld last-member-query-interval

ipv6 mld last-member-query-interval

Configures the IPv6 MLDv1 snooping last-member query interval on a specific VLAN interface.

Syntax

ipv6 mld last-member-query-interval *msec*

no ipv6 mld last-member-query-interval

Parameters

msec

The range is from 100 through 2500 milliseconds. The default is 1000.

Modes

Interface subtype configuration mode

Usage Guidelines

The last-member query interval is the interval for the response to a query sent after a host leave message is received from the last known active host on the subnet. The group is deleted if no reports are received in this interval. This interval adjusts the speed at which messages are transmited on the subnet. Smaller values detect the loss of a group member faster.

Use the **no** form of this command to restore the default.

Examples

To configure IPv6 MLDv1 snooping last-member query interval on a VLAN interface:

```
switch(config)# int vlan 2000
switch(config Vlan-2000)# ipv6 mld last-member-query-interval 25
```

Related Commands

ipv6 mld last-member-query-count

ipv6 mld query-interval

Configures the maximum interval for IPv6 MLDv1 snooping queries for a specific VLAN interface.

Syntax

ipv6 mld query-interval *sec*

no ipv6 mld query-interval

Parameters

sec

The range is from 1 through 18000 seconds. The default is 125.

Modes

Interface subtype configuration mode

Usage Guidelines

The value set by the **ipv6 mld query-interval** command must be greater than the value set by the **ipv6 mld query-max-response-time** command.

A larger value means that queries are sent less often.

Use the **no** form of this command to restore the default.

Examples

To configure the maximum interval for IPv6 MLDv1 snooping queries on a VLAN interface:

```
switch(config)# int vlan 2000
switch(config Vlan-2000)# ipv6 mld query-interval 1200
```

Related Commands

ipv6 mld query-max-response-time

ipv6 mld query-max-response-time

Configures the maximum response time for IPv6 MLDv1 snooping queries for a specific VLAN interface.

Syntax

ipv6 mld query-max-response-time *sec*

no ipv6 mld last-member-query-interval

Parameters

sec

The range is 1 through 25 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

The maximum response delay is inserted into the periodic general query interval. This is useful when snooping querier functionality is enabled. Larger values spread out host responses over a longer time.

The value set by the **ipv6 mld query-max-response-time** command must be less than the value of the general query interval that is set by the **ipv6 mld query-interval** command.

Use the **no** form of this command to restore the default.

Examples

To configure IPv6 MLDv1 query maximum response time on a VLAN interface:

```
switch(config)# int vlan 2000
switch(config Vlan-2000)# ipv6 mld query-max-response-time 15
```

Related Commands

ipv6 mld query-interval

ipv6 mld snooping enable

Enables IPv6 MLDv1 Layer 2 snooping globally or on a specific VLAN.

Syntax

ipv6 mld snooping enable

no ipv6 mld snooping enable

Command Default

IPv6 MLDv1 snooping is disabled.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

MLD snooping must be enabled globally first, after which it must be enabled on a VLAN

Use the **no** form of this command to disable IPv6 MLDv1 snooping globally or on a specific VLAN.

NOTE
When MLD snooping is disabled globally, the snooping configuration remains in the running configuration and snooping is disabled on all VLANs.

Examples

To enable IPv6 MLDv1 snooping globally:

```
switch(config)# ipv6 mld snooping enable
```

To enable IPv6 MLDv1 snooping on a specific VLAN:

```
switch(config)# int vlan 10
switch(config-Vlan-10)# ipv6 mld snooping enable
```

ipv6 mld snooping fast-leave

Configures the immediate-leave feature for the groups on a specific VLAN.

Syntax

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

This command minimizes the leave latency of group memberships on an interface, as the device does not send group-specific queries. As a result, the group entry is removed from the multicast routing table as soon as a group leave message is received.

Use the **no** form of this command to restore the default.

Examples

To configure the immediate-leave feature on a VLAN:

```
switch(config)# int vlan 2000
switch(config-Vlan-2000)# ipv6 mld snooping fast-leave
```

ipv6 mld snooping mrouter interface

Configures a VLAN port member to be a multicast router (mrouter) port.

Syntax

ipv6 mld snooping mrouter interface { <*N*>**gigabitethernet** | **port-channel** *number* }

no ipv6 mld snooping mrouter interface { <*N*>**gigabitethernet** | **port-channel** *number* }

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the port-channel number. The number of available channels ranges from 1 through 6144.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to disable the VLAN port member from being an mrouter port.

Examples

To configure a VLAN port member to be an mrouter port:

```
switch(config)# int vlan 2000
switch(config-Vlan-2000)# ipv6 mld snooping interface te 54/0/1
```

ipv6 mld snooping querier enable

Activates or deactivates IPv6 MLDv1 Layer 2 multicast snooping querier functionality for a VLAN.

Syntax

ipv6 mld snooping querier enable

no ipv6 mld snooping querier enable

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to deactivate this functionality.

Examples

To enable MLD snooping querier functionality on a VLAN:

```
switch(config)# int vlan 2000
switch(config-Vlan-2000)# ipv6 mld snooping querier enable
```

ipv6 mld snooping restrict-unknown-multicast

Deactivates or reactivates on a VLAN the flooding of unregistered multicast data traffic on IPv6 MLDv1 snooping-enabled VLANs.

Syntax

ipv6 mld snooping restrict-unknown-multicast

no ipv6 mld snooping restrict-unknown-multicast

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

MLD snooping must be enabled globally first, after which it must be enabled on a VLAN.

Use the **no** form of this command to reactivate the flooding of unregistered multicast data traffic on all IPv6 MLDv1 snooping-enabled VLANs.

NOTE
When MLD snooping is disabled globally, the snooping configuration remains in the running configuration and snooping is disabled on all VLANs.

Examples

To deactivate on a VLAN the flooding of unregistered multicast data traffic:

```
switch(config-Vlan-2000)# ipv6 mld snooping restrict-unknown-multicast
```

To reactivate on a VLAN the flooding of unregistered multicast data traffic :

```
switch(config-Vlan-2000)# no ipv6 mld snooping restrict-unknown-multicast
```

ipv6 mld snooping robustness-variable

Configures a value to compensate for packet loss in congested networks.

Syntax

ipv6 mld snooping robustness-variable *value*

no ipv6 mld snooping robustness-variable *value*

Command Default

This feature is disabled.

Parameters

value

The range is from 2 through 10. The default is 2.

Modes

Interface subtype configuration mode

Usage Guidelines

This value determines the number of general MLD snooping queries that are sent before a multicast address is aged out for lack of a response.

Use the **no** form of this command to restore the default.

Examples

To change the robustness variable from the default on a VLAN:

```
switch(config-Vlan-2000)# ipv6 mld snooping robustness-variable 7
```

ipv6 mld startup-query-count

Configures the IPv6 MLDv1 number of queries that are separated by the startup query interval.

Syntax

ipv6 mld startup-query-count *value*

no ipv6 mld startup-query-count *value*

Command Default

This feature is disabled.

Parameters

value

The range is from 1 through 10. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To change the startup query count on a VLAN:

```
switch(config-Vlan-2000)# ipv6 mld startup-query-count 5
```

Related Commands

ipv6 mld startup-query-interval

ipv6 mld startup-query-interval

Configures the IPv6 MLDv1 startup query interval.

Syntax

ipv6 mld startup-query-interval *value*

no ipv6 mld startup-query-interval *value*

Command Default

This feature is disabled.

Parameters

value

The range is from 1 through 450. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To change the startup query interval on a VLAN:

```
switch(config-Vlan-2000)# ipv6 mld startup-query-interval 4
```

Related Commands

ipv6 mld startup-query-count

ipv6 mld static-group interface

Configures IPv6 MLDv1 Layer 2 multicast static IPv6 groups on an interface for a VLAN.

Syntax

ipv6 mld static-group *group-IPv6-address* **interface** *interface*

no ipv6 mld static-group *group-IPv6-address* **interface** *interface*

Parameters

group-IPv6-address
A multicast address to be joined, in the format *xxxx:xxxx/ml, xxxx:xxxx::/ml*

interface
An Ethernet or port-channel interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to remove the static-group configuration on an interface for a VLAN.

Examples

To configure multicast static IPv6 groups on an Ethernet interface for a VLAN:

```
switch(config)# int vlan 2000
switch(config-Vlan-2000)# ipv6 mld static-group ff1e::1 interface te 54/0/1
```

ipv6 mtu

Configures a maximum size for IPv6 MTU packets to be sent on an interface.

Syntax

ipv6 mtu *bytes*

no ipv6 mtu

Parameters

bytes

IPv6 MTU in bytes. Range is from 576 through 9018. The default is 1500.

Modes

RBridge ID configuration mode

Interface subtype configuration mode

Usage Guidelines

To route packets larger than 2500 bytes (the default for an Ethernet interface), you must also use the **mtu** command to set the same MTU value on the interface as that set by the **ipv6 mtu** command. Otherwise packets will be dropped. The range for the **mtu** command is from 1522 through 9219 bytes.

Use the **no** form of this command to restore the default.

Examples

To configure a maximum MTU size of 1800 on an Ethernet interface:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# int te 3/0/1
switch(config-if-int-te-3/0/1)# ipv6 mtu 1800
```

ipv6 nd cache expire

Configures the time interval after which the IPv6 Neighbor Discovery cache is deleted or refreshed.

Syntax

ipv6 nd cache expire *minutes*

no ipv6 nd cache expire *minutes*

Parameters

minutes

Interval in minutes. The range is from 1 through 240. The default is 240.

Modes

RBridge ID configuration mode

Interface subtype configuration mode

Usage Guidelines

Cache entries expire and are deleted if they remain in a "stale" state as defined by *minutes*.

Use the **no** version of this command to restore the default interval at whch the cache is deleted.

Examples

To set the Neighbor Discovery cache deletion or refresh interval to 180 minutes on an Ethernet interface:

```
switch(config)# rbridge-id 54
switch(config-rbridge-id-54)# int te 54/0/3
switch(config-if-te-54/0/3)# ipv6 nd cache expire 180
```

ipv6 nd dad attempts

Configures the number of IPv6 Neighbor Discovery Neighbor Solicitation (NS) messages to be sent as part of duplicate address detection (DAD).

Syntax

ipv6 nd dad attempts *number*

no ipv6 nd dad attempts *number*

Parameters

number

Number of solicitations. The range is from 0 through 10. The default is 2.

Modes

RBridge ID configuration mode

Interface subtype configuration mode

Usage Guidelines

To restore the number of neighbor solicitation messages to be sent to the default value, use the **no** form of this command.

Examples

To set the number of Neighbor Discovery NS messages to be sent on an Ethernet interface to 5:

```
switch(config)# rbridge-id 54
switch(confg-rbridge-id-54)# int te 54/0/3
switch(config-if-te-54/0/3)# ipv6 nd dad attempts 5
```

To disable DAD on an Ethernet interface:

```
switch(config)# rbridge-id 54
switch(confg-rbridge-id-54)# int te 54/0/3
switch(config-if-te-54/0/3)# ipv6 nd dad attempts 0
```

ipv6 nd dad time

Configures the retransmit time interval for IPv6 Neighbor Discovery Neighbor Solicitation (NS) messages that are sent as part of duplicate address detection (DAD).

Syntax

ipv6 nd dad time *seconds*

no ipv6 nd dad time

Parameters

seconds

Time in seconds. The range is from 1 through 5. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

To restore the default NS message retransmit interval for DAD, use the **no** form of this command.

Use the **ipv6 nd ns-interval** command to configure the interval for NS address resolution.

Examples

To set the retransmit time interval globally for Neighbor Discovery NS messages to be sent on a specified RBridge to 3 seconds:

```
switch(config-rbridge-id-122)# ipv6 nd dad time 3
```

To set the retransmit time interval for Neighbor Discovery NS messages to be sent on an Ethenet interface to 3 seconds:

```
switch(config)# rbridge-id 54
switch(config-rbridge-id-54)# int te 54/0/3
switch(config-if-te-54/0/3)# ipv6 nd dad time 3
```

Related Commands

ipv6 nd ns-interval

ipv6 nd hoplimit

Configures the number of hops to be advertised in IPv6 Neighbor Discovery Router Advertisement (RA) messages.

Syntax

ipv6 nd hoplimit *number*

no ipv6 nd hoplimit

Parameters

number

The number of hops to be advertised. The range is from 0 through 255. The default is 64.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To set the number of hops to be advertised in Neighbor Discovery RA messages sent on an Ethernet interface to 32:

```
switch(config-if-te-54/0/3)# ipv6 nd hoplimit 32
```

ipv6 nd managed-config-flag

In IPv6 Neighbor Discovery, indicates to hosts on a local link that they must use the stateful autoconfiguration feature to obtain IPv6 addresses for their interfaces.

Syntax

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Modes

Interface subtype configuration mode

Usage Guidelines

If the **ipv6 nd managed-config-flag** command is configured, hosts use stateful autoconfiguration to obtain IPv6 address information.

- If the **ipv6 nd managed-config-flag** command is configured, it overrides an existing configuration set by the **ipv6 nd other-config-flag** command.
- If the **ipv6 nd managed-config-flag** command is not configured, whether hosts can obtain IPv6 addresses by means of the stateful autoconfiguration feature is determined by means of the **ipv6 nd other-config-flag** command.

Use the **no** form of this command to remove the configuration.

Examples

To indicate to hosts on a local link to an Ethernet interface that they must use the stateful autoconfiguration feature to obtain IPv6 addresses for their interfaces:

```
switch(config-if-te-54/0/3)# ipv6 nd managed-config-flag
```

Related Commands

ipv6 nd other-config-flag

ipv6 nd mtu

Sets the size of the maximum transmission unit (MTU) that is advertised in Neighhbor Discovery Router Advertisement (RA) messages.

Syntax

ipv6 nd mtu *number*

no ipv6 nd mtu

Parameters

number

Size, in bytes, of the MTU that is advertised. The range is from 1280 through 65535. The default is 1500.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To set the maximum IPv6 MTU packet size to 2400 bytes on an Ethernet interface:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# int te 3/1/1
switch(config-if-te-3/1/1)# ipv6 nd mtu 2400
```

ipv6 nd ns-interval

Sets the interval for address resolution between IPv6 Neighbor Discovery Neighbor Solicitation (NS) messages.

Syntax

ipv6 nd ns-interval *seconds*

no ipv6 nd ns-interval

Parameters

seconds

Number of seconds between neighbor solicitation messages. The range is from 1 through 5. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

This command sets the interval for address resolution only. Use the **ipv6 nd dad time** command to configure the retransmit time interval for NS messages that are sent as part of duplicate address detection (DAD) .

Use the **no** form of this command to restore the default.

Examples

To set the interval between Neighbor Discovery NS messages sent on an Ethernet interface to 3 seconds:

```
switch(config-if-te-54/0/3)# ipv6 nd ns-interval 3
```

Related Commands

ipv6 nd dad time

ipv6 nd other-config-flag

In IPv6 Neighbor Discovery, indicates to hosts on a local link that they can use the stateful autoconfiguration feature to obtain configuration settings other than IPv6 address information for their interfaces.

Syntax

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Modes

Interface subtype configuration mode

Usage Guidelines

If the **ipv6 nd managed-config-flag** command is configured, local hosts use stateful autoconfiguration to obtain IPv6 addresses for their interfaces.

- If the **ipv6 nd managed-config-flag** command is configured, it overrides an existing configuration set by the **ipv6 nd other-config-flag** command.
- If the **ipv6 nd managed-config-flag** command is not configured, whether hosts can obtain IPv6 address information by means of the stateful autoconfiguration feature is determined by means of the **ipv6 nd other-config-flag** command.

Use the **no** form of this command to remove the configuration.

Examples

To indicate to local hosts on an Ethernet interface that they must use the stateful autoconfiguration feature to obtain configuration settings other than IPv6 address information for their interfaces:

```
switch(config-if-te-54/0/3)# ipv6 nd other-config-flag
```

Related Commands

ipv6 nd managed-config-flag

ipv6 nd prefix

Configures which IPv6 prefixes are included in IPv6 Neighbor Discovery Router Advertisement (RA) messages.

Syntax

ipv6 nd prefix *ipv6-prefix/prefix-length*

no ipv6 nd prefix *ipv6-prefix/prefix-length*

Parameters

ipv6-prefix
IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to remove the IPv6 prefixes.

Valid and preferred lifetimes are default values, which are 2592000 and 604800, respectively.

Examples

To include an IPv6 prefix in router advertisement messages sent out an Ethernet interface:

```
switch(config-if-te-54/0/3)# ipv6 nd prefix 2ffe:1111::/64
```

ipv6 nd ra-interval

Configures the maximum interval range and minimum interval at which IPv6 Neighbor Discovery Router Advertisement (RA) messages are sent.

Syntax

ipv6 nd ra-interval *max-value* **min** *min-value*

no ipv6 nd ra-interval

Parameters

max-value

Maximum interval range in seconds. The range is from 4 through 1800. The defaut is interval is 200 through 600, with messages sent randomly within that interval.

min

Specifies a minimum interval in seconds.

min-value

The range is from 0 through 1800. The default is 200.

Modes

Interface subtype configuration mode

Usage Guidelines

It is recommended that the interval set by this command be less than or equal to the device lifetime value set by the **ipv6 nd ra-lifetime** command if the device is advertised as a default device.

Use the **no** form of this command to restore the default.

Examples

To set a maximum interval range and minimum interval for RA messages on an Ethernet interface:

```
switch(config-if-te-54/0/3)# ipv6 nd ra-interval 1200 min 400
```

Related Commands

ipv6 nd ra-lifetime

ipv6 nd ra-lifetime

Configures the amount of time in IPv6 Neighbor Discovery that a router is considered a valid default router.

Syntax

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameters

seconds

Time in seconds. The range is from 0 through 9000. The defaut is 1800.

Modes

Interface subtype configuration mode

Usage Guidelines

Note the following behavior:

- If the value set by this command is 0, the router is not advertised as a default router on the interface.
- If the value set by this command is not 0, the router is considered a default router on the interface.

It is recommended that the interval set by this command be greater than or equal to the value set by the **ipv6 nd ra-interval** command if the device is advertised as a default device.

Use the **no** form of this command to restore the default.

Examples

To set the time that a router is considered a valid default router on an Ehernet interface:

```
switch(config-if-te-54/0/3)# ipv6 nd ra-lifetime 2400
```

Related Commands

ipv6 nd ra-interval

ipv6 nd reachable-time

Configures the amount of time in IPv6 Neighbor Discovery that a deivce considers a remove IPv6 node reachable.

Syntax

ipv6 nd reachable-time milli *seconds*

no ipv6 nd reachable-time

Parameters

milliseconds

Time in milliseconds. The range is from 0 through 3600000. The defaut is 0.

Modes

Interface subtype configuration mode

Usage Guidelines

Setting the reachable time to a nonzero value ensures that all nodes on the same link share the same value. The default of 0 means that no reachable time specified.

Use the **no** form of this command to restore the default.

Examples

To set the amount of time that a deivce considers a remove IPv6 node reachable on an Ethernet interface:

```
switch(config-if-te-54/0/3)# ipv6 nd reachable-time 1800000
```

ipv6 nd retrans-timer

Configures the time advertised between IPv6 Neighbor Discovery Neighbor Solicitation (NS) messages.

Syntax

ipv6 nd retrans-timer *milliseconds*

no ipv6 nd retrans-timer

Parameters

milliseconds

Interval, in milliseconds, at which NS messages are sent. The range is from 0 through 4294967295. The default is 0.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To set the time advertised between NS messages on an interface:

```
switch(config-if-te-54/0/3)# ipv6 nd retrans-timer 4500000
```

ipv6 nd suppress-ra

Disables the sending of ICMPv6 Router Advertisement (RA) messages, including those sent in response to a solicitation as well as MTUs.

Syntax

ipv6 nd suppress-ra [**all** | **mtu**]

no ipv6 nd suppress-ra [**all** | **mtu**]

Parameters

all

Disables the sending of all RA messages, including those sent in response to a solicitation.

mtu

Disables the sending of MTUs in RA messages.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to enable the sending of RA messages.

Examples

To disable the sending of RA messages on an Ethernet interface, but allowing those sent in response to a solicitation:

```
switch(config-if-te-54/0/3)# ipv6 nd suppress-ra
```

To disable the sending of RA messages, as well as those sent in response to a solicitation:

```
switch(config-if-te-54/0/3)# ipv6 nd suppress-ra all
```

To disable the sending of RA messages, allowing those sent in response to a solicitation, but also disabling the sending of MTUs:

```
switch(config-if-te-54/0/3)# ipv6 nd suppress-ra mtu
```

ipv6 neighbor

Configures the IPv6 and MAC addresses of a neighbor as static entries for IPv6 Neighbor Discovery.

Syntax

ipv6 neighbor *ipv6address MACaddress*

no ipv6 neighbor

Parameters

ipv6address
IPv6 address of a neighbor in *A:B:C:D* format.

MACaddress
MAC address of the neighbor in *HHHH.HHHH.HHHH* format.

Modes

RBridge ID configuration mode.

Usage Guidelines

Use the **no** form of this command to remove the IPv6 and MAC addresses.

Examples

The following configures an IPv6 and MAC address on an Ethernet interface for a neighbor:

```
switch(config)# rbridge-id 54
switch(config-rbridge-id-54)# ipv6 neighbor 2001:0db8:8086:6501::/32 abcd.abcd.abcd
```

ipv6 ospf active

Sets a specific OSPFv3 interface to active.

Syntax

ipv6 ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ipv6 ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

Examples

To set a specific OSPFv3 virtual Ethernet (VE) interface to active:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# interface ve 95
device(config-Ve-95)# ipv6 ospf active
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf area

Enables OSPFv3 on an interface.

Syntax

ipv6 ospf area *area-id* | *ipv6-addr*

no ipv6 ospf area

Command Default

OSPFv3 is disabled.

Parameters

area-id

Area address in dotted decimal or decimal format.

ipv6-addr

IPv6 address.

Modes

Interface subtype configuration mode

Usage Guidelines

This command enables an OSPFv3 area on the interface to which you are connected.

Enter **no ipv6 ospf area** to disable OSPFv3 on this interface.

Examples

To enable a configured OSPFv3 area named 0 on a specific OSPFv3 10-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf area 0
```

To enable a configured OSPFv3 area named 0 on a specific OSPFv3 virtual Ethernet (VE) interface:

```
device(config)# rbridge-id 177
device(config-rbridge-id-177)# interface ve 12
device(config-ve-12)# ipv6 ospf area 0
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf authentication ipsec

Specifies IPsec as the authentication type for an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec key-add-remove-interval *interval*

no ipv6 ospf authentication ipsec key-add-remove-interval *interval*

Command Default

Authentication is disabled.

Parameters

key-add-remove-interval *interval*

Specifies the OSPFv3 authentication key add-remove interval. Valid values range from decimal numbers 0 through 14400. The default is 300.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf authentication ipsec** to remove IPsec authentication from the interface.

Examples

To enable IPsec on a specified OSPFv3 10-gigabit interface:

```
device# configure
device(config)# interface te 1/0/1
device(config-if-te-1/0/1)# ipv6 ospf area 0
device(config-if-te-1/0/1)# ipv6 ospf authentication ipsec
```

To set the OSPFv3 authentication key add-remove interval to 480:

```
device# configure
device(config)# interface te 1/0/1
device(config-if-te-1/0/1)# ipv6 ospf area 0
device(config-if-te-1/0/1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```

History

Release version	Command history
5.0.1a	This command was introduced.

ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec disable

no ipv6 ospf authentication ipsec disable

Command Default

Authentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf authentication ipsec** to re-enable IPSec on the interface if IPsec is already configured on the interface.

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPSec encapsulated and the received packets which are IPSec encapsulated will be dropped.

Examples

To disable IPsec on a specific OSPFv3 10-gigabit Ethernet interface where IPsec is already enabled:

```
device# configure
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf authentication ipsec disable
```

History

Release version	Command history
5.0.1a	This command was introduced.

ipv6 ospf authentication spi

Specifies the security policy index (SPI) value for an OSPFv3 interface.

Syntax

ipv6 ospf authentication spi *spi* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** [**no-encrypt**] *key* }

no ipv6 ospf authentication spi

Command Default

Authentication is disabled.

The 40 hexadecimal character key is encrypted by default. Use the **no-encrypt** parameter to disable encryption.

Parameters

spi
SPI value. Valid values range from decimal numbers 512 through 4294967295.

ah
Specifies Authentication Header (ah) as the protocol to provide packet-level security.

esp
Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null
Specifies that the ESP payload is not encrypted.

hmac-md5
Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF interface.

hmac-sha1
Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF interface.

key
Number used in the calculation of the message digest. The 40 hexadecimal character key is stored in encrypted format by default.

no-encrypt
The 40-character key is not encrypted upon either its entry or its display.

key
The 40 hexadecimal character key.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf authentication spi** *spi* to remove the SPI value from the interface.

Examples

To enable ESP and HMAC-SHA-1 on a specified OSPFv3 10-gigabit interface:

```
device# configure
device(config)# interface Te 1/0/1
device(config-if-te-1/0/1)# ipv6 ospf area 0
device(config-if-te-1/0/1)# ipv6 ospf authentication spi 512 esp null hmac-sha1 key
abcef12345678901234fedcba098765432109876
```

To enable HA and HMAC-MD5 on a specified OSPFv3 10-gigabit interface:

```
device# configure
device(config)# interface Te 1/0/1
device(config-if-te-1/0/1)# ipv6 ospf area 0
device(config-if-te-1/0/1)# ipv6 ospf authentication spi 750 ha hmac-md5 key
abcef12345678901234fedcba098765432109876
```

History

Release version	Command history
5.0.1a	This command was introduced.

ipv6 ospf cost

Configures cost for a specific interface.

Syntax

ipv6 ospf cost *value*

no ipv6 ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the **auto-cost reference-bandwidth** command.

Enter **no ipv6 ospf cost** to disable this configuration.

Examples

To set the cost to 550 on a specific OSPFv3 10-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf cost 550
```

To set the cost to 620 on a specific IPv6 OSPF Virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# rbridge-id 177
device(config-rbridge-id-177)# interface ve 14
device(config-ve-14)# ipv6 ospf cost 620
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ipv6 ospf dead-interval *interval*

no ipv6 ospf dead-interval

Command Default

40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to be one fourth of the new dead interval, unless the hello interval is also explicitly configured using the **ipv6 ospf hello-interval** command. The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that is automatically changed as the result of a dead-interval change is not displayed.

Enter **no ipv6 ospf dead-interval** to use the default value.

Examples

To set the dead interval to 60 on a specific IPv6 OSPF 40-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface fortygigabitethernet 101/0/10
device(conf-if-fo-101/0/10)# ipv6 ospf dead-interval 60
```

To set the dead interval to 80 on a specific IPv6 OSPF virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# interface ve 24
device(config-ve-24)# ipv6 ospf dead-interval 80
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

Syntax

ipv6 ospf hello-interval *interval*

no ipv6 ospf hello-interval

Command Default

10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to be four times the new hello interval, unless the dead interval is also explicitly configured using the **ipv6 ospf dead-interval** command. The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that is automatically changed as the result of a hello-interval change is not displayed.

Enter **no ipv6 ospf hello-interval** to use the default value.

Examples

To set the hello interval to 150 on a specific OSPFv3 40-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface fortygigabitethernet 101/0/10
device(conf-if-fo-101/0/10)# ipv6 ospf hello-interval 150
```

To set the hello interval to 220 on a specific OSPFv3 virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# interface ve 24
device(config-ve-24)# ipv6 ospf hello-interval 220
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

Syntax

ipv6 ospf hello-jitter *interval*

no ipv6 ospf hello-jitter

Parameters

jitter

Allowed interval between hello packets.Valid values range from 1 through 50 percent (%).

Modes

Interface subtype configuration mode

Usage Guidelines

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

Examples

To set the hello jitter to 20 on a specific OSPFv3 40-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface fortygigabitethernet 101/0/20
device(conf-if-fo-101/0/10)# ipv6 ospf hello-jitter 20
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf instance

Specifies the number of OSPFv3 instances running on an interface.

Syntax

ipv6 ospf instance *instanceID*

no ipv6 ospf instance

Parameters

instanceID

Instance identification number. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode .

Usage Guidelines

Enter **no ipv6 ospf instance** to use the default value.

Examples

To set the number of IPv6 OSPF instances to 35 on a specific OSPFv3 40-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface fortygigabitethernet 101/0/20
device(conf-if-fo-101/0/10)# ipv6 ospf instance 35
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Command Default

Enabled

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv3 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

Enter **no ipv6 ospf mtu-ignore** to disable MTU-match checking on a specific interface.

Examples

To disable MTU-match checking on a specific IPv6 OSPF 40-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface fortygigabitethernet 101/0/10
device(conf-if-fo-101/0/10)# no ipv6 ospf mtu-ignore
```

To disable MTU-match checking on a specific IPv6 OSPF virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# rbridge-id 177
device(config-rbridge-id-171778)# interface ve 24
device(config-ve-24)# no ipv6 ospf mtu-ignore
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf network

Configures network type.

Syntax

ipv6 ospf network { **broadcast** | **point-to-point** }

no ipv6 ospf network

Command Default

Network type is broadcast.

Parameters

broadcast
Network type is broadcast, such as Ethernet.

point-to-point
Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

Enter **no ipv6 ospf network** to remove the network-type configuration.

NOTE
The network type non-broadcast is not supported at this time.

Examples

To configure an OSPFv3 point-to-point link on the OSPFv3 10-gigabit Ethernet interface whose rbridge-ID/slot/port format is 190/0/49:

```
device# configure terminal
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf network point-to-point
```

To configure an OSPFv3 broadcast link on the OSPFv3 virtual Ethernet (VE) interface 20:

```
device# configure terminal
device(config)# rbridge-id 178
device(config-rbridge-id-178)# interface ve 20
device(config-ve-20)# ipv6 ospf network broadcast
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf passive

Sets a specific OSPFv3 interface to passive.

Syntax

ipv6 ospf passive

no ipv6 ospf passive

Modes

Interface subtype configuration mode

Usage Guidelines

The **ipv6 ospf passive** command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

Examples

To set a specific OSPFv3 virtual Ethernet (VE) interface to passive:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# int ve 200
device(config-Ve-200)# ipv6 ospf passive
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

ipv6 ospf active

ipv6 ospf priority

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

Syntax

ipv6 ospf priority *value*

no ipv6 ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

Enter **no ipv6 ospf priority** to use the default value.

Examples

To set a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 10-gigabit Ethernet interface 190/0/49:

```
device# configure terminal
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf priority 4
```

To set a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 virtual Ethernet (VE) interface 27:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# interface ve 27
device(config-ve-27)# ipv6 ospf priority 4
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf retransmit-interval

Configures retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface

Syntax

ipv6 ospf retransmit-interval *rtx-int*

no ipv6 ospf retransmit-interval

Command Default

5 seconds.

Parameters

rtx-int

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ip ospf retransmit-interval** to reset the retransmit interval to its default.

Examples

To set the retransmit interval to 8 for all OSPFv3 routers on the OS-gigabit Ethernet interface 190/0/49:

```
device# configure terminal
device(config)# interface tengigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf retransmit-interval 8
```

To set the retransmit interval to 26 for all OSPFv3 routers on the OSPFv3 virtual Ethernet (VE) interface 22:

```
device# configure terminal
device(config)# rbridge-id 178
device(config-rbridge-id-178)# interface ve 22
device(config-ve-22)# ipv6 ospf retransmit-interval 26
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf suppress-linklsa

Suppresses link LSA advertisements.

Syntax

ipv6 ospf suppress-linklsa

no ipv6 ospf suppress-linklsa

Modes

Interface subtype configuration mode

Examples

To suppress link LSAs from being advertised on routers on the OSPFv3 40-gigabit Ethernet interface 190/0/49:

```
device# configure terminal
device(config)# interface fortygigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf suppress-linklsa
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmiot delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

Syntax

ipv6 ospf transmit-delay *tx-delay*

no ipv6 ospf transmit-delay

Command Default

1 second.

Parameters

tx-delay

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf transmit-delay** to use the default value.

Examples

To set a transmit delay of 25 seconds for routers on the OSPFv3 40-gigabit Ethernet interface 190/0/49:

```
device# configure terminal
device(config)# interface fortygigabitethernet 190/0/49
device(conf-if-te-190/0/49)# ipv6 ospf transmit-delay 25
```

To set a transmit delay of 45 seconds for routers on the OSPFv3 virtual Ethernet (VE) interface 22:

```
device# configure terminal
device(config)# rbridge-id 177
device(config-rbridge-id-177)# interface ve 22
device(config-ve-22)# ipv6 ospf transmit-delay 43
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 prefix-list

Configures IPv6 prefix lists for use in basic traffic filtering.

Syntax

ipv6 prefix-list *name* [**seq** *sequence-number*] **deny** *ipv6-prefix/prefix-length* | **permit** *ipv6-prefix/prefix-length* | **description** *string* [**ge** *ge-value*] [**le** *le-value*]

no ipv6 prefix-list *name*

Parameters

name

Specifies the prefix list name. You use this name when using the prefix list as input to command or route map.

seq *sequence-number*

Specifies the IPv6 prefix list's sequence number. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with prefix list entry 5. The Brocade device interprets the prefix list entries in numerical order, beginning with the lowest sequence number.

deny *ipv6-prefix/prefix-length*

This parameter denies a packet if the packet contains a route specified in the prefix list. The prefix list matches only on the specified i *pv6-prefix/prefix-length* unless you use the **ge** *ge-value* or **le** *le-value* parameters.

permit *ipv6-prefix/prefix-length*

This parameter permits a packet if the packet contains a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length unless you use the **ge** *ge-value* or **le** *le-value* parameters.

description *string*

This parameter is a text string describing the prefix list.

ge *ge-value*

If you specify only **ge** *ge-value*, then the range is from ge-value to 128.

le *le-value*

If you specify only **le** *le-value*, then the range is from *le-value* to the *prefix-length* parameter.

Modes

Global configuration mode

Usage Guidelines

An IPv6 prefix list is composed of one or more conditional statements that execute a permit or deny action if a packet matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When a Brocade device interface sends or receives an IPv6 packet, it applies the statements within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the device takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature. You can configure up to one hundred IPv6 prefix lists.

Use the **no ipv6 prefix-list** *name* command to delete a prefix list.

You must specify the ipv6-prefix parameter in hexadecimal using 16-bit values between colons as documented in RFC 4291. You must specify the prefix-length parameter as a decimal value. A slash mark (/) must follow the ipv6-prefix parameter and precede the prefix-length parameter.

The *ge-value* or *le-value* you specify must meet the following condition for the prefix-length:

```
ge-value <= le-value <= 128
```

If you do not specify **ge** *ge-value* or **le** *le-value*, the prefix list matches only on the exact prefix you specify with the *ipv6-prefix/prefix-length* parameter.

Examples

To configure an IPv6 prefix list and use it as input to the RIPng **distribute-list** command, enter the following commands.

```
switch(config)# ipv6 prefix-list routesfor2001 permit 2001::/16
switch(config)# ipv6 router rip
switch(config-ripng-router)# distribute-list prefix-list routesfor2001 out ethernet 3/1
```

These commands permit the inclusion of routes with the IPv6 prefix 2001::/16 in RIPng routing updates sent from Ethernet interface 3/1.

Related Commands

ipv6 address, distribute-list route-map

ipv6 protocol vrrp

Globally enables IPv6 VRRPv3.

Syntax

ipv6 protocol vrrp

no ipv6 protocol vrrp

Command Default

Disabled

Modes

RBridge ID configuration mode

Usage Guidelines

The **no ipv6 protocol vrrp** command globally disables VRRPv3.

Examples

To enable IPv6 VRRPv3 globally:

```
switch# configure
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 protocol vrrp
```

Related Commands

ipv6 protocol vrrp-extended

ipv6 protocol vrrp-extended

Globally enables IPv6 VRRP-Ev3.

Syntax

ipv6 protocol vrrp-extended

no ipv6 protocol vrrp-extended

Command Default

Disabled

Modes

RBridge ID configuration mode

Usage Guidelines

The **no ipv6 protocol vrrp-extended** command globally disables IPv6 VRRP-Ev3.

Examples

To enable IPv6 VRRP-Ev3 globally:

```
switch# configure
switch (config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 protocol vrrp-extended
```

Related Commands

ipv6 protocol vrrp

ipv6 route

Configures a static IPv6 route for an interface, with a destination network, a next-hop gateway, and an optional administrative distance.

Syntax

ipv6 route *dest-ipv6-prefix/prefix-length* [*next-hop-ipv6-address* | *link-local-next-hop-ipv6-address*] [*<N>***gigabitethernet** *slot/port* | **null 0** | **ve** *vlan_id*] [*metric*] [**distance** *number*] [**tag** *tag*]

ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address*

no ipv6 route *dest-ipv6-prefix/prefix-length* [*next-hop-ipv6-address* | *link-local-next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag*]

no ipv6 route *dest-ipv6-prefix/prefix-length* [*next-hop-ipv6-address* | *link-local-next-hop-ipv6-address*] [*<N>***gigabitethernet** *rbridge-id/slot/port* | **null 0** | **ve** *vlan_id*] [*metric*] [**distance** *number*] [**tag** *tag*]

no ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address*

Command Default

See Parameter defaults.

Parameters

dest-ipv6-prefix
Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

next-hop-ipv6-address
IPv6 address of the next-hop gateway.

link-local-next-hop-ipv6-address
IPv6 address of the link-local next-hop gateway.

next-hop-vrf *vrf_namenext-hop-ipv6-address*
Specifies a VRF instance and a next-hop IPv6 address.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

null 0
Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

ve *vlan_id*

Specifies the VLAN ID of a virtual Ethernet (VE) interface.

metric

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has numberalready placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance

Specifies an administrative distance. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route.

number

The range is from 1 through 255. The default is 1.

tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag

A number from 0 through 4294967295. The default is 0.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to configure a static IPv6 route for an interface, with a destination network, a next-hop gateway, and an optional administrative distance.

Examples

To configure a static IPv6 route to a destination network with the prefix 2001:db8::0/32, a next-hop gateway with the global address 2001:db8:0:ee44::1, and an administrative distance of 110:

```
switch(rbridge-id-54)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 distance 110
```

NOTE

See the Brocade Network OS Administration Guide for additional examples and details.

ipv6 router ospf

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol over VRF.

Syntax

ipv6 router ospf [**vrf** *name*]

no ipv6 router ospf

Command Default

This command is disabled by default.

Parameters

vrf *name*

The name of the non-default VRF to connect.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 VRF router configuration mode. OSPFv3 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

Enter **no ipv6 router ospf** to delete all current OSPFv3 configuration and to block any further OSPFv3 configuration. If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Examples

To enable OSPFv3 on a default VRF and to enter IPv6 OSPF VRF router configuration mode:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)#ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)#
```

History

Release version	Command history
5.0.0	This command was introduced.

ipv6 unreachable

Prohibits routers from forwarding an Internet Control Message Protocol version 6 (ICMPv6) Destination Unreachable Code 3 (port unreachable) message on a point-to-point link back onto the ingress port.

Syntax

ipv6 unreachable

no ipv6 unreachable

Command Default

This command is enabled by default.

Modes

Global configuration mode

Usage Guidelines

By default, ICMPv6 Destination Unreachable Code 3 messages are sent for a discarded IP packet. You can disable the sending of these messages. Use the **no ipv6 unreachable** command to disable the sending of these messages.

This is an interface-specific configuration The configuration is persistent across a switch reload.

Related Commands

ip unreachable

ipv6 vrrp-extended-group

Configures an IPv6 VRRP-Ev3 group and enters into the VRRP-E configuration mode.

Syntax

ipv6 vrrp-extended-group *group-ID*

no ipv6 vrrp-extended-group *group-ID*

Parameters

group-ID

A number from 1 through 128 that you assign to the VRRP-Ev3 group.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-extended-group** *group-ID* to remove the specific IPv6 VRRP-Ev3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

This configuration is for virtual Ethernet (VE) interfaces only. IPv6 VRRP-Ev3 must be enabled on the device before the IPv6 VRRP-E group is configured.

Examples

The following example shows how to assign the VE interface with a VLAN number of 2019 to the VRRP-Ev3 group with the ID of 19.

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 protocol vrrp-extended
switch(config-rbridge-id-122)# interface ve 2019
switch(config-Ve-2019)# ipv6 address 2001:2019:8192::122/64
switch(config-Ve-2019)# ipv6 vrrp-extended-group 19
switch(config-vrrp-extended-group-19)#
```

Related Commands

ipv6 protocol vrrp-extended

ipv6 vrrp-group

Configures an IPv6 VRRPv3 group and enters into the virtual router configuration mode.

Syntax

ipv6 vrrp-group *group-ID*

no ipv6 vrrp-group *group-ID*

Parameters

group-ID

A value from 1 through 128 that you assign to the VRRPv3 group.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-group** *group-ID* to remove a specific IPv6 VRRPv3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

IPv6 VRRPv3 must be enabled on the device before the IPv6 VRRP group is configured.

Examples

The following example shows how to assign the 10-gigabit Ethernet interface 101/1/6 to the VRRPv3 group with the ID of 18.

```
switch(config)# rbridge-id 125
switch(config-rbridge-id-125)# ipv6 protocol vrrp
switch(config-rbridge-id-125)# interface tengigabitethernet 101/1/6
switch(config-if-te-101/1/6)# ipv6 address 2001:2019:8192::125/64
switch(config-if-te-101/1/6)# ipv6 vrrp-group 18
switch(config-vrrp-group-18)#
```

Related Commands

ipv6 protocol vrrp

ipv6 vrrp-suppress-interface-ra

Suppresses interface router advertisement (RA) when VRRPv3 is configured on an interface.

Syntax

ipv6 vrrp-suppress-interface-ra

no ipv6 vrrp-suppress-interface-ra

Command Default

Disabled

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-suppress-interface-ra** to remove the suppression of interface RA.

Router advertisements are sent by the VRRP master device and contain the link-local virtual IP address and the virtual MAC address. For network security reasons, if you do not want the MAC addresses of interfaces to be viewed, you can disable RA messages.

Examples

This example suppresses interface RA on a virtual Ethernet (VE) interface:

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 protocol vrrp
switch(config-rbridge-id-122)# interface ve 2019
switch(config-Ve-2019)# ipv6 vrrp-suppress-interface-ra
```

iscsi-priority

Sets the iSCSI priority bitmap for use in the DCBX iSCSI TLV.

Syntax

iscsi-priority *value*

no iscsi-priority

Command Default

Priority bitmap value is 4.

Parameters

value

The priority bitmap value. Valid values range from 0 through 7.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no iscsi-priority** to return to the default value.

isl-r_rdy

Sets the flow control primitive used to prevent frame drop to ISL R_RDY mode.

Syntax

isl-r_rdy

no isl-r_rdy

Command Default

no isl-r_rdy or VC_RDY flow control mode.

Modes

Interface Fibre Channel configuration mode

Usage Guidelines

ISL R_RDY mode can be enabled only for a port configured for long distance operation with long distance modes LE, LD, or LS.

In ISL R_RDY mode, the port sends the R_RDY primitive signal that the port is ready to receive frames. The port sends an exchange link parameter (ELP) with flow control mode 02. If a port is ISL R_RDY enabled, it can only receive an ELP with flow control mode 02. A received ELP with flow control mode 01 will segment the fabric.

Brocade recommends disabling ISL R_RDY.

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6740 switches), in Brocade VCS Fabric mode, and with the FCoE license installed.

A Fibre Channel port configured as a trunk port cannot have the ISL R_RDY flow control enabled.

Enter **no isl-r_rdy** to disable ISL R_RDY mode on a port, and instead establish VC_RDY flow control.

Examples

To enable ISL R_RDY mode on a port:

```
switch(config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# isl-r_rdy
```

To disable ISL R_RDY mode on a port:

```
switch(config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# no isl-r_rdy
```

keep-alive timeout (fabric-map)

Enables or disables the keep-alive timeout.

Syntax

keep-alive timeout

no keep-alive timeout

Modes

FCoE fabric-map configuration mode

Usage Guidelines

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

Enter **no keep-alive timeout** to disable the keep-alive timeout.

Related Commands

fabric-map, fcoe

key-add-remove-interval

Alters the timing of the authentication key add-remove interval.

Syntax

key-add-remove-interval *interval*

no key-add-remove-interval *interval*

Command Default

The interval is 300 seconds.

Parameters

interval

Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no key-add-remove-interval** to set the add-remove interval to the default value of 300 seconds.

Examples

To set the key add-remove interval to 240 seconds:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-add-remove-interval 240
```

To set the key add-remove interval to 210 seconds in a nondefault VRF instance:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf vrf vrf_1
device(config-ipv6-router-ospf-vrf-vrf_1))# key-add-remove-interval 240
```

History

Release version	Command history
5.0.1a	This command was introduced.

key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

key-rollover-interval *interval*

no key-rollover-interval *interval*

Command Default

The interval is 300 seconds.

Parameters

interval

Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no key-rollover-interval** to set the rollover interval to the default value of 300 seconds. In order to have consistent security parameters, rekeying should be done on all nodes at the same time. Use the **key-rollover-interval** command to facilitate this. The key rollover timer waits for a specified period of time before switching to the new set of keys. Use this command to ensure that all the nodes switch to the new set of keys at the same time.

Examples

To set the key rollover interval to 420 seconds:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-rollover-interval 420
```

To re-set the key rollover interval to the default value:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no key-rollover-interval
```

To re-set the key rollover interval to the default value in a nondefault VRF instance:

```
device# configure
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf vrf vrf_1
device(config-ipv6-router-ospf-vrf-vrf_1))# no key-rollover-interval
```

History

Release version	Command history
5.0.1a	This command was introduced.

l2traceroute

This command sends a simple traceroute from the source MAC address to the destination MAC address.

Syntax

l2traceroute

Modes

Privileged EXEC mode

Usage Guidelines

This command does not support command-line parameters. You are prompted for the required information after you enter the **l2traceroute** command.

This command sends a plain Layer 2 traceroute, hop by hop, from the switch that learned the source MAC address to the switch that learned the destination MAC address. The IP parameters included in the **l2traceroute** command allow for generating frames with similar properties as the ones generated from a connected device, thus traversing the same path through the fabric.

Configuration results depend on the configuration parameters specified. The following fields display when you enter the **l2traceroute** command:

- Source MAC address—Enter the source MAC address. The MAC address must be a valid MAC address that exists in the mac-address-table.
- Destination MAC address—Enter the destination MAC address. The MAC address must be a valid MAC address that exists in the mac-address-table.
- Vlan—Enter the VLAN number. On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:
  - On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
  - On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- Edge rbridge-id—Enter the edge RBridge ID on which the **l2traceroute** command is to run.
- Extended commands—Enter **Y** to enable extended commands, which include protocol type (IP or FCoE), source IP address, destination IP address, IP protocol type (TCP or UDP), source port number, and destination port number.

Based on the input for Extended commands, if you enter **Y** , the parameters branch as follows:

- Protocol Type [IP]—Enter the protocol type. You must select the IP including.
  - Source IP address—Enter the source IP address.
  - Destination IP address—Enter the destination IP address.
- IP Protocol Type [**TCP** | **UDP**| **0-255**]—Enter the IP protocol type including:
  - TCP (Transmission Control Protocol) is a connection-oriented protocol, which means that it requires handshaking to set up end-to-end communications.

  - UDP (User Datagram Protocol) is a message-based connectionless protocol. Communication occurs by transmitting information in one direction, from the source to the destination, without verifying the readiness of the receiver.
  - 0-255 is the numeric protocol value. to use as filter.
- The source port number. The valid port range is 0 through 65535. This is an optional field.
- The destination port number. The valid port range is 0 through 65535. This is an optional field.

Examples

This example shows extended commands, IP protocol type, and TCP as the IP protocol type.

```
switch# l2traceroute

Source mac address                : 0050.564f.549f
Destination mac address           : 0005.1ea0.8dd8
Vlan [1-3583]                     : 1
Edge rbridge-id [1-239]           : 1
Extended commands [Y/N]?          : Y
Protocol Type [IP/FCoE]           : IP
Source IP address                 : 192.85.1.2
Destination IP address            : 192.0.2.2
IP Protocol Type [TCP/UDP/0-255]  : TCP
Source port number [0-65535]      : 58
Dest port number [0-65535]        : 67
switch# l2traceroute

Source mac address                : 0000.0000.1111
Destination mac address           : 0000.0000.2222
Vlan [1-3583]                     : 1
Edge rbridge-id [1-239]           : 50
Extended commands [Y/N]?          : n
Rbridge    Ingress                   Egress                    Rtt(usec)
-------------------------------------------------------------------------------
50         Te 50/0/15                Te 50/0/38(isl)           0
40         Te 40/0/38(isl)           Te 40/0/2(isl)            60322
10         Te 10/0/2(isl)            Te 10/0/4(isl)            1274
20         Te 20/0/4(isl)            Te 20/0/10(isl)           1119
30         Te 30/0/10(isl)           Te 30/0/19                1787
```

lacp default-up

Activates an LACP link in the absence of PDUs.

Syntax

lacp default-up

no lacp default-up

Modes

Interface subtype configuration mode

Usage Guidelines

This command forces the port to activate an LACP link if there are no PDUs available on the interface port.

This command is supported on all physical interfaces.

This command is visible only if the interface is a dynamic and standard member of a port-channel.

This command is not supported on Static LAGs.

This command is not supported on static or dynamic Brocade Trunks.

This command is not supported on any other types of interfaces, such as port-channel or VLAN.

Enter **no lacp default-up** to disable this feature.

Examples

```
switch# (conf-if-te-1/0/9)# lacp default-up
```

lacp port-priority

Sets the priority of the physical interface for LACP.

Syntax

lacp port-priority *value*

no lacp port-priority

Command Default

The default value is 32768.

Parameters

value

Specifies the priority. Valid values range from 1 through 65535. A lower number takes priority over a higher number.

Modes

Interface subtype configuration mode.

Usage Guidelines

An LACP port priority is configured on each port using LACP. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

A link with higher priority (smaller in value) gets preference over a link with lower priority (greater in value).

Enter **no lacp port-priority** to return to the default value.

Examples

To set the LACP port priority to 1000 for a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9

switch(conf-if-te-178/0/9)# lacp port-priority 1000
```

Related Commands

interface

lacp system-priority

Sets the Link Aggregation Control Protocol (LACP) system priority. The LACP priority determines which system is responsible for resolving conflicts in the choice of aggregation groups.

Syntax

lacp system-priority *value*

no lacp system-priority

Command Default

The default value is 32768.

Parameters

value

Specifies the value of the LACP system priority. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Lower numerical values have higher priorities.

Enter **no lacp system-priority** to reset the system priority to the default value.

Examples

To set the LACP system-priority to 68:

```
switch(config)# lacp system-priority 68
```

To clear the configured LACP system-priority:

```
switch(config)# no lacp system-priority
```

lacp timeout

Sets the timeout value used by the Link Aggregation Control Protocol (LACP) to exchange packets on an interface before invalidating a received data unit (DU).

Syntax

lacp timeout { **long** | **short** }

no lacp timeout

Command Default

For Brocade trunks, the default value is the **short** timeout.

For standard LAGs, the default value is the **long** timeout.

Parameters

long

Specifies that a long-timeout value of 30 seconds will be used. With this value, the port waits three times this long (90 seconds) before invalidating the information received earlier on this PDU.

short

Specifies that a short-timeout value of one second will be used. With this value, the port waits three times this long (three seconds) before invalidating the information received earlier on this PDU.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set the timeout value based on how frequently you think the switch will receive LACP PDUs from the partner switch.

Enter **no lacp timeout** to return to the default values.

Examples

To use the LACP long-timeout value on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9

switch(conf-if-te-178/0/9)# lacp timeout long
```

Related Commands

interface

ldap-server host

Configures an LDAP-server host.

Syntax

ldap-server host { *ipaddr* | *FQDN* } [**port** *portnum*] [**domain** *basedn*] [**timeout** *secs*] [**retries** *num*]

no ldap-server host { *ipaddr* | *FQDN* }

Command Default

- Timeout: 5 seconds
- Port: 389
- Retries: 5

Parameters

ipaddr | *FQDN*
Specifies the IPv4 address or Fully Qualified Domain name of the Active Directory (AD) server. IPv6 is supported for Windows 2008 AD server only. The maximum supported length for the LDAP host name is 40 characters.

port *portnum*
Specifies the TCP port used to connect the AD server for authentication. The port range is from 1024 through 65535.

domain *basedn*
Describes the base domain name of the host.

timeout *secs*
Specifies the wait time for a server to respond. The range is 1 through 60 seconds.

retries *num*
Specifies the number of retries for the server connection. The range is 0 through 100.

Modes

Global configuration mode

Usage Guidelines

Use this command to sets up a connection to the Lightweight Directory Access Protocol (LDAP) server host, or modifies an existing configuration. A maximum of 5 LDAP servers can be configured on a switch. Executing "no" on an attribute sets it with its default value.

Enter **no ldap-server host** to delete the server configuration.

Enter **no ldap-server host** with a parameter to restore the default value for that parameter.

Invoking **no** on an attribute sets the attribute with its default value.

Examples

To add an LDAP server on port 3890 with retries set to three:

```
switch(config)# ldap-server host 10.24.65.6 domain sec.brocade.com port 3890 retries 3
```

To change the domain in an existing configuration:

```
switch(config)# ldap-server host 10.24.65.6

switch(config-host-10.24.65.6)# domain security.brocade.com
```

To delete an LDAP server:

```
switch(config)# no ldap-server host 10.24.65.6
```

To reset the number of retries to the default value:

```
switch(config)# ldap-server host 10.24.65.6 retries
```

Executing **no** on an attribute sets it with its default value.

```
switch(config)# no ldap-server host 10.24.65.6 retries
```

Attributes holding default values will not be displayed.

```
switch# show running-config ldap-server host 10.24.65.6

ldap-server host 10.24.65.6
 port      3890
 domain        security.brocade.com
```

Related Commands

certutil import ldapca, ldap-server maprole, show running-config ldap-server

ldap-server maprole

Maps an Active Directory (AD) group to a switch role.

Syntax

ldap-server maprole group *group_name* **role** *role_name*

no ldap-server maprole group *group_name*

Parameters

group *group_name*
The name of the AD group.

role *role_name*
The name of the switch role.

Modes

Global configuration mode

Usage Guidelines

Enter **no ldap-server maprolegroup** *group_name* without the **role** *role_name* parameter to remove the mapping of the AD group to a role.

Examples

To map the AD group "Administrator" to the switch role "admin":

```
switch(config)# ldap-server maprole group Administrator role admin
```

To remove the mapping:

```
switch(config)# no ldap-server maprole group Administrator
```

Related Commands

certutil import ldapca, ldap-server host, show running-config ldap-server

license add

Adds a license key to a switch.

Syntax

license add { **licstr** *licenseString* | **FTP-URL** *ftpPath* | **SCP-URL** *scpPath* } [**rbridge-id** *rbridge-id*]

Command Default

This command is executed on the local switch.

Parameters

licstr *licenseString*
Specifies the license string to be added to the switch. The license string must be enclosed in double quotation marks. A maximum of 256 characters is allowed.

FTP-URL *ftpPath*
Specifies a URL from which to transfer license information using FTP. ftp://*username*:*password*@*hostname filepath*

SCP-URL *scpPath*
Specifies a URL from which to transfer license information using SCP. scp://*username*:*password*@*hostname*/ *filepath*

rbridge-id *rbridge-id*
Executes the command on the remote switch specified by the RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Depending on the feature being added, you may need to disable and re-enable the affected ports for this command to take effect. Follow the instructions in the command output.

If you install a license on an unsupported platform, the operation succeeds, but the **show license** output indicates that the license is not supported.

In the Network OS v3.0.0 release, this command is supported only on the local RBridge.

Examples

To add a license on the local switch:

```
switch# license add licstr "*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#"

Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

To add a Dynamic Ports on Demand (DPOD) license on a switch that does not support the feature:

```
switch# license add licstr "*B
a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDXxFgbB3f2w3pJNlujxLVdIVkX
doNHf6i4SzwuvimIj0ORN:JOojLU#"

License Added [*B
a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDXxFgbB3f2w3pJNlujxLVdIVkX
doNHf6i4SzwuvimIj0ORN:JOojLU#]
switch# show license

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Ports on Demand license - not applicable on this platform license
Feature name:PORTS_ON_DEMAND_1
    License is valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Related Commands

license remove, show license, show license id

license remove

Removes a license key from a switch or deactivates a temporary license that cannot be removed..

Syntax

license remove licstr { *licenseString* | *feature* } [**rbridge-id** *ID*]

Command Default

This command is executed on the local switch.

Parameters

licstr *licenseString*

Removes the specified license string and associated feature. The license string must be enclosed in double quotation marks.

licstr *feature*

Removes the license string associated with the specified feature from the license database of the local switch. The feature name must be enclosed in double quotation marks. Supported licensed features include the following: FCOE_BASE, PORTS_ON_DEMAND_1, PORTS_ON_DEMAND_2, VCS_FABRIC, ADVANCED_SERVICES, LAYER_3, PORT_10G_UPGRADE and PORT_0G_UPGRADE.

rbridge-id *ID*

Executes the command on the remote switch specified by the RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

You cannot display the license string once you install it. If you do not remember the string, use the feature name displayed in the **show license** command output to remove the license.

Depending on the feature being removed you must first clear all license-related configurations, and possibly disable and re-enable selected ports for this command to take effect. Follow the instructions in the command output.

This command deactivates but does not permanently remove time-based trial licenses.

You must disable or remove all configurations related to a licensed feature before you can remove the license for that feature. To remove the 10G and 40G Port Upgrade licenses, you must remove all non-Base-allowance port reservations for the respective license type.

In the Network OS v3.0.0 release this command is supported only on the local RBridge.

Examples

To remove a license string from the local switch:

```
switch# license remove licstr "*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#

Removing license for rbridge-id 2 [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

To remove a license based on the feature name from the local switch:

```
switch# license remove licstr "FCOE_BASE"

removing license feature name [FCOE_BASE]
```

Related Commands

license add, show license, show license id

line vty exec-timeout

Sets the CLI session timeout.

Syntax

line vty exec-timeout *timeout*

no line vty exec-timeout

Command Default

The default timeout value is 10 minutes.

Parameters

timeout

Specifies the CLI session timeout period in minutes. The timeout value specifies the amount of time a CLI session can be idle before it logs you out. Valid values range from 0 through 136.

Modes

Global configuration mode

Usage Guidelines

The **line vty exec timeout** command is a configuration command and the timeout value set by this command holds for subsequent login sessions, unless it is overwritten for a single session with the **terminal timeout** command. The terminal timeout command is not a configuration command and the timeout value set by this command controls only the current session. After the current session times out, the **line vty exec timeout** value applies for subsequent sessions.

This command is supported only on the local switch.

This command is not available on the standby management module.

Enter **no line vty exec-timeout** to disable auto-logout and delete the timeout value.

Examples

To set the terminal timeout to 60 minutes:

```
switch(config)# line vty exec-timeout 60

switch(config-line-vty)# exit

switch(config)# exit

switch# show running-config line vty

line vty
exec-timeout 60
!
```

Related Commands

terminal

linecard

Configures a line card (interface module).

Syntax

linecard *slot_number linecard_type*

no linecard *slot_number*

Parameters

slot_number

Specifies the slot number to be configured. Line card slots are slots 1 through 4 on a Brocade VDX 8770-4 and slots 1 through 8 on a Brocade VDX 8770-8.

linecard_type

Specifies the type of line card. Enter **linecard** *slot_number linecard_type* **?** to display currently supported types.

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

Use this command to configure the specified slot for an line card of a given type.

The command is executed in the context of the given RBridge. You must first enter the rbridge-id context for the specific line card. Once you are in the rbridge-id context, enter **linecard***slot_number linecard_type* to configure the slot. If you replace a given line card with another one of a different type, you must remove the configuration and then reconfigure the slot.

The line card must be powered off before you can remove the slot configuration.

The LC72x1G type displayed under "possible completion" is not supported.

CAUTION

Enter no linecard to remove the slot configuration. When hot-swapping line cards of different types, copy the running-config file to the startup-config file before rebooting. This ensures that the desired changes are persistent in case there are any hardware or software incompatibilities.

Examples

To configure a slot for an line card on a switch in VCS mode and to verify the configuration:

```
switch# configure

Entering configuration mode terminal
switch(config)# rbridge-id 1

switch(config-rbridge-id-1)# linecard 1 ?

Possible completions:
  LC12x40G   12X40G linecard
  LC48x1G    48X1G linecard
  LC48x10G   48X10G linecard
  LC72x1G    72X1G linecard
switch(config-rbridge-id-1)# linecard 1 LC48x10G

Creating new linecard configuration was successful.
switch(config-rbridge-id-1)# do show running-config rbridge-id 1 linecard

rbridge-id 1
  linecard 1 LC48x10G
  linecard 4 LC48x10G
```

Related Commands

show running-config rbridge-id linecard

lldp dcbx-version

Specifies which version of the Data Center Bridging Exchange (DCBX) protocol to use.

Syntax

lldp dcbx-version { **auto** | **cee** }

no lldp dcbx-version

Command Default

The default setting is **auto**.

Parameters

auto

Specifies to auto-adjust the DCBX protocol version to accommodate the difference when a switch interacts with different vendors using a different version of the DCBX protocol.

cee

Specifies to use the Converged Enhanced Ethernet (CEE) DCBX version.

Modes

Interface subtype configuration mode

Usage Guidelines

Devices enabled for data center bridging can use the DCBX protocol to discover and exchange information about their administratively configured capabilities. DCBX eliminates the need to configure a large number of switches in the network.

Enter **no lldp dcbx-version** to return to the default setting.

Examples

To specify that the CEE version be used on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp dcbx-version cee
```

Related Commands

interface, lldp disable, lldp iscsi-priority, lldp profile

lldp disable

Disables the Link Layer Discovery Protocol (LLDP) on the interface.

Syntax

lldp disable

no lldp disable

Command Default

LLDP is enabled at both the global and interface levels.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no lldp disable** to enable LLDP on a specific interface.

Examples

To disable LLDP on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp disable
```

To enable LLDP on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# no lldp disable
```

lldp iscsi-priority

Sets the priority that will be advertised in the DCBX iSCSI TLV for a specified interface.

Syntax

lldp iscsi-priority *value*

no lldp iscsi-priority

Command Default

Priority value is 4.

Parameters

value

Specifies the priority value. Valid values range from 0 through 7.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no lldp iscsi-priority** to return to the default setting.

Examples

To set the iSCSI priority value to 5 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# lldp iscsi-priority 5
```

lldp profile

Applies a Link Layer Discovery Protocol (LLDP) profile to an interface.

Syntax

lldp profile *name*

no lldp profile

Command Default

LLDP profile name.

Parameters

name

Specifies the profile name. Valid profile name length is between 1 and 32 characters.

Modes

Interface subtype configuration mode

Usage Guidelines

You must use the **lldp profile** command to create an LLDP profile before you can apply the profile to the interface. Only one LLDP profile can exist at any time for a particular interface. When this command is not present, the parameters defined in the global LLDP configuration are used.

Enter **no lldp profile** to delete the profile from the interface.

Examples

To apply an LLDP profile called *test* on an specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9

switch(conf-if-te-178/0/9)# lldp profile test
```

load-balance

Configures load balancing settings.

Syntax

load-balance [**dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-mac-vid-port** | **src-dst-ip-port** | **src-dst-mac-vid** | **src-mac-vid**]

no load-balance

Command Default

The default setting is the operand *src-dst-ip-mac-vid-port*, which means that source and destination IP, MAC address, VID and TCP/UDP port-based load balancing are used.

Parameters

dst-mac-vid
Specifies that destination MAC address and VID-based load balancing will be used.

src-dst-ip
Specifies that source and destination IP address-based load balancing will be used.

src-dst-ip-mac-vid
Specifies that source and destination IP and MAC address and VID-based load balancing will be used.

src-dst-ip-mac-vid-port
Specifies that source and destination IP, MAC address, VID and TCP/UDP port-based load balancing will be used. This is the default.

src-dst-ip-port
Specifies that source and destination IP and TCP/UDP port-based load balancing will be used.

src-dst-mac-vid
Specifies that source and destination MAC address and VID-based load balancing will be used.

src-mac-vid
Specifies that source MAC address and VID-based load balancing will be used.

Modes

Port-channel configuration mode

Usage Guidelines

Use the **no** form of this command to return to the default setting.

When configuring load balancing on a Brocade VDX 6740, it should be configured consistently for all port-channels on the switch. These switches support one load-balancing scheme at a time, and apply the last loaded load-balancing scheme to all port-channels on the switch. This is not required for the Brocade VDX 8770 platform, as it supports multiple port-channel load-balancing schemes.

Examples

To set load balancing to use the destination MAC address and VID-based load balancing:

```
switch# configure
switch(config)# interface port-channel 10
switch(config-Port-channel-10)# load balance dst-mac-vid
```

load-balancing

Configures load balancing.

Syntax

load-balancing threshold-priority *threshold-priority-value*

no load-balancing

Command Default

None

Parameters

threshold-priority *threshold-priority-value*
The load balancing threshold priority. The range is from 1 through 254.

Modes

Fabric-Virtual-Gateway on an RBridge VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command to remove the threshold priority value.

Examples

The following example shows how to configure load balancing.

```
switch(config)# rbridge-id  1
switch(config-rbridge-id-1)# interface ve 2000
switch(config-rbridge-Ve-2000)# ip fabric-virtual-gateway 23
switch(config-ip-fabric-virtual-gw)# load-balancing threshold-priority 100
```

History

Release version	Command history
5.0.1	This command was introduced.

load-balancing-disable

Disables load balancing.

Syntax

load-balancing-disable

no load-balancing-disable

Command Default

Load balancing is enabled.

Modes

Fabric-Virtual-Gateway in VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command to re-enable load balancing.

Examples

The following example shows how to disable load balancing.

```
switch(config)# interface ve 2000
switch(config-Ve-2000)# ip fabric-virtual-gateway
switch(config-ip-fabric-virtual-gw)# load-balancing-disable
```

History

Release version	Command history
5.0.1	This command was introduced.

local-as (BGP)

Specifies the autonomous system number (ASN) where the device resides.

Syntax

local-as *num*

no local-as

Parameters

num

The local ASN. The range is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

The ASN for associates a given device it with other devices in its autonomous system.

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

Use the **no** form of this command to remove the ASN from the device.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# local-as 777
```

log-dampening-debug

Logs dampening debug messages.

Syntax

log-dampening-debug

no log-dampening-debug

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# log-dampening-debug
```

log-status-change

Controls the generation of all OSPFv3 logs.

Syntax

log-status-change

no log-status-change

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of events related to OSPFv3, such as neighbor state changes and database overflow conditions.

Use the **no** form of this command to restore the default.

Examples

To disable the logging of events:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no log-status-change
```

To enable the logging of events:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log-status-change
```

History

Release version	Command history
5.0.0	This command was introduced.

logging auditlog class

Sets the severity levels (class) for the audit log class.

Syntax

logging auditlog class *class*

no logging auditlog class *class*

Command Default

CONFIGURATION, FIRMWARE, and SECURITY audit log classes are enabled.

Parameters

class

Specifies the class name of the audit log. Valid classes are CONFIGURATION, FIRMWARE, and SECURITY.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

The total message storage available is 2048 messages.

Enter **no logging auditlog class** *class* to remove the audit logging for the specified class.

Related Commands

clear logging auditlog, clear logging raslog

logging raslog console

Sets the severity levels for the RASLog console and allows users to temporarily stop showing RASLog messages on the console.

Syntax

logging raslog console *severity*

no logging raslog console *severity*

logging raslog console stop [*minutes*]

Command Default

Severity level is INFO.

Parameters

severity

Specifies the minimum severity level of the message to pass through the filter. Valid values consist of one of the following: INFO, WARNING, ERROR, or CRITICAL. Input values are case-sensitive.

start

Initiates RASLog messages.

stop

Stops RASLog messages.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

The total message storage available is 2048 messages.

When stopping or starting RASLog messages, the commands are not persistent and therefore are not configuration commands.

If the command **logging raslog console stop** *minutes* is invoked before the previous time value expires, the latest CLI duration applies.

Examples

To reset the RASLog severity levels to the default value.

```
switch(config)# no logging raslog console
```

To stop RASLog messages for 1 minute:

```
switch# logging raslog console stop 1
Logging message have been blocked on console for 1 minutes
```

To start RASLog messages:

```
switch# logging raslog console start

2013/11/14-08:42:57, [RAS-3008], 5348, M2 | Active, INFO, VDX8770-4, Logging messages to console has
been reset by user.
```

Related Commands

clear logging raslog, show running-config logging

logging syslog-facility local

Configures the syslog facility.

Syntax

logging syslog-facility local *log_level*

Command Default

Syslog level is LOG_LOCAL7.

Parameters

log_level

Specifies the syslog facility level. Valid log levels include the following: LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the log level for all error log entries to forward to one or more specified servers. You can configure up to four servers.

When used without a log level parameter, use this command to display the current value.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To configure the syslog facility level:

```
switch(config)# logging syslog-facility local LOG_LOCAL5
```

Related Commands

logging syslog-server, show running-config logging syslog-server

logging syslog-server

Configures a switch to forward system messages to specified servers.

Syntax

logging syslog-server *ip_address* [**secure** { **true** | **false** }] [**port** [*value*]]

no logging syslog-server *ip_address*

Command Default

If the secure parameter is set to **true** and the port number is not specified, the default port number of 6514 is used.

The default value for the secure parameter is **false**.

Parameters

ip_address

Specifies the IP address of the syslog server in IPv4 or IPv6 format.

secure{**true**|**false**

} Configures a secure syslog server. A secure port number with default values is not shown in the Brocade Network OS database.

port*value*

Configures the port for the syslog server.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a switch to forward all error log entries to the one or more specified servers. You can configure up to four servers.

The **certutil import syslogca** command is required for secure syslog to be fully functionalou can configure up to four syslog servers. You must execute the command for each server.

This command is not supported on the standby management module.

In a Brocade VCS Fabric, the syslog configuration is distributed to all switches in the fabric.

If the secure parameter is set to **false**, you are not able to set the port number.

Enter **no logging syslog-server** to remove the specified IP address.

Examples

To configure a server to which system messages are sent:

```
switch(config)# logging syslog-server 192.168.163.233
```

To remove a configured syslog server:

```
switch(config)# no logging syslog-server 192.168.163.233
```

To remove a syslog server port:

```
switch(config)# no logging syslog-server 10.17.17.203 secure port 1999
switch(config)# do show running-config logging syslog-server
logging syslog-server 10.17.17.203
secure
```

Related Commands

certutil import syslogca, logging syslog-facility local, show running-config logging syslog-facility, show running-config logging syslog-server

logical-chassis principal-priority

Sets the priority of a switch to assign a specific RBridge ID the role of principal node in a logical chassis cluster.

Syntax

logical-chassis principal-priority *priority-value*

no logical-chassis principal-priority

Parameters

priority-value
Sets the priority for the switch. A lower number means a higher priority. Values range from 1 through 128.

Modes

RBridge ID configuration mode

Usage Guidelines

If all switches boot up at the same time, the default priority is the same and all switches will compare their mutual intents. The switch with the lowest switch WWN becomes the principal switch. However, you can use this command to select the principal switch in a logical chassis cluster. For this command to take effect, you need to issue the **logical-chassis principal-switchover** command.

This command can be used only on nodes that are part of a logical chassis cluster. The node, however, can be disconnected from the cluster when you issue the command.

Use the **no** form of this command to remove a priority value from this node.

You can view the principal priority in both the **show running config** (using the **rbridge-id** operand) and **show vcs detail** command outputs (both are run in Privileged EXEC mode).

Examples

To set the principal priority to 5 for switch that is in logical chassis cluster:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# logical-chassis principal-priority 5
```

Related Commands

logical-chassis principal-switchover

logical-chassis principal-switchover

Triggers a fabric reformation and elects a principal node based on the principal priority value.

Syntax

logical-chassis principal-switchover

Modes

Privileged EXEC mode

Usage Guidelines

Issue this command after you have used the **logical-chassis principal-priority** *priority-value* command so that the priority you set takes effect and a new principal node is selected on the cluster.

Examples

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# logical-chassis principal-priority 1
switch(config-rbridge-id-5)# end
switch# logical-chassis principal-switchover
```

Related Commands

logical-chassis principal-priority

long-distance-isl

Extends an ISL link up to 30 km.

Syntax

long-distance-isl { **2000** | **5000** | **10000** | **30000** }

no long-distance-isl

Command Default

The default is 2 km.

Parameters

2000

Specifies a 2 km distant link.

5000

Specifies a 5 km distant link.

10000

Specifies a 10 km distant link.

30000

Specifies a 30 km distant link. DCB/FCoE capabilities are not supported with this setting.

Modes

Interface subtype configuration mode

Usage Guidelines

Metro VCS supports long-distance ISL ports up to 30 km on the Brocade VDX platforms listed below. Links up to 10 km are lossless. You can have eight 1-km links forming a Brocade trunk. You can also have mixed length cables forming the ISL. For ECMP purposes, you can have eight 8-link ECMP trunks.

TABLE 6 Limitations for long-distance Metro VCS

Supported hardware	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Brocade VDX 6740	yes	yes	yes	yes
Brocade VDX 8770 - VDX LC48x10G line card	yes	yes	yes	yes

The following displays the limitations on extended ISL for Network OS hardware.

TABLE 7 Conditions for long distance Metro VCS

Condition	Extended ISLup to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Support for lossless FCoE/iSCSI traffic on the Metro VCS port-group	yes	yes	yes	no
Layer 2/IP Lossy Traffic support	yes	yes	yes	yes
Number of Metro VCS long distance ports supported per port group	1	1	1	1
Number of regular ISLs supported on a port group configured for long distance	1	1	0	0
Trunking support between multiple LD ISLs	no	no	no	no
CEE map or FCoE port allowed in same port-group	no	no	no	no
eNS Sync (MAC address table sync)	yes	yes	yes	yes
Zoning	yes	yes	yes	yes
HA failover	yes	yes	yes	yes
Node redundancy check	yes	yes	yes	yes
vMotion	yes	yes	yes	yes
Maximum PFCs Supported	3 (2 on the Brocade VDX 6740)	3(2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)
Long-distance ISL on 40G to 4x10G breakout interfaces	no	no	no	no
Long-distance ISL on 1G and 10G copper interfaces	no	no	no	no

The following displays the port groups and number of port groups available on each platform for long distance Metro VCS.

TABLE 8 Long distance Metro VCS port-group schema

Platform	Port groups	Number of port groups on platform
Brocade VDX 6740	1-32, 33-48 (49-50 do not support long distance)	2*
Brocade VDX 8770 (VDX LC48x10G linecard)	1-8, 9-16, 17-24, 25-32, 33-40, 41-48	6 per LCX10G blade

*Not a valid deployment scenario at distances longer than 5 km, as no normal ISLs are allowed if both port-groups are configured with long-distance ISLs for 10 km and 30 km.For a 10 km ISL link, no other ISL links are allowed on the same ASIC.

For 2 km and 5 km ISL links, another short distance ISL link can be configured.

A maximum of three PFCs can be supported on a long distance ISL link.

Enter **no long-distance-isl** to revert to the default value.

Examples

To extend the support of an ISL port with PFC by a distance of 5 km on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9

switch(conf-if-te-178/0/9)# long-distance-isl 5000
```

Related Commands

interface, isl-r_rdy

mac

Allows the user to add a MAC address to a MAC address group in a service or transport VF configuration supporting multitenancy in a Virtual Fabrics context.

Syntax

mac *mac_address*

no mac *mac_address*

Parameters

mac_address
Specifies a MAC address in dot-separated hexadecimal notation.

Modes

MAC group configuration mode

Usage Guidelines

Use this command in MAC group configuration mode to add a MAC address to a MAC address group in a service or transport VF configuration supporting multitenancy in a Virtual Fabrics context.

Enter the MAC group configuration mode by using the **mac group** *mac-group-id* global configuration command.

Enter **no mac** *mac_address* to remove a MAC addresses from the group.

NOTE
You can add or remove only one MAC address per line.

Examples

To enter MAC group configuration mode and add a MAC address to the group:

```
switch(config)# mac-group 1
switch(config-mac-group 1)# mac abc1.abc2.abc3
```

To remove a MAC address from the group:

```
switch(config-mac-group 1)# no mac abc1.abc2.abc3
```

Related Commands

mac-group, vcs virtual-fabric enable

mac access-group

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

mac access-group *ACLname* { **in** | **out** }

no mac access-group *ACLname* { **in** | **out** }

Parameters

ACLname
Specifies the name of the standard or extended MAC access list.

in
Specifies to filter inbound packets only.

out
Specifies to filter outbound packets only.

Modes

Interface-subtype configuration mode

Usage Guidelines

You can apply a maximum of two Layer 2 ACLs to a user interface, as follows:

- One ingress MAC ACL
- One egress MAC ACL

NOTE
You can apply an ACL to multiple interfaces. And you can apply an extended ACL twice—ingress and egress—to a given user interface.

To remove a MAC ACL from an interface, enter the **no** form of this command.

Examples

The following example applies an ingress MAC ACL named macacl2, and to filter inbound packets only, on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# mac access-group macacl2 in
```

The following example removes an ingress MAC ACL named macacl2 from a specific port-channel interface:

```
switch(config)# interface port-channel 62
switch(conf-port-channel-62)# no mac access-group macacl2 in
```

Related Commands

interface, mac access-list extended, mac access-list standard

mac access-list extended

Creates an extended MAC access control list (ACL). An extended ACL contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

mac access-list extended *ACLname*

no mac access-list extended *ACLname*

Parameters

ACLname

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

Use this command to create an extended MAC access list. If the ACL is already created, this command puts the switch in the extended MAC access-list configuration mode.

Extended ACLs allow you to filter traffic based on the following:

- Source MAC address
- Destination MAC address
- EtherType

You can apply named MAC extended ACLs to VLANs and to Layer 2 interfaces.

Standard and extended MAC ACLs cannot share the same name.

To remove a MAC ACL from an interface, enter the **no** form of this command.

Examples

The following example creates a MAC extended ACL named mac1:

```
switch(config)# mac access-list extended mac1
switch(conf-macl-ext)#
```

The following example deletes a MAC extended ACL named mac1:

```
switch(conf-macl-ext)# no mac access-list extended mac1
```

mac access-list standard

Creates a standard MAC access control list (ACL). Standard ACLs contain rules that permit or deny traffic based on source addresses that you specify.

Syntax

mac access-list standard *ACLname*

no mac access-list standard *ACLname*

Parameters

ACLname

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a standard MAC access list. If ACL is already created, this command puts the switch in the standard MAC access-list configuration mode.

Standard and extended MAC ACLs cannot share the same name.

To remove a MAC ACL from an interface, enter the **no** form of this command.

Examples

The following example creates a MAC standard ACL named mac1:

```
switch(config)# mac access-list standard mac1
switch(conf-macl-std)#
```

The following example deletes a MAC standard ACL named mac1:

```
switch(conf-macl-std)# no mac access-list standard mac1
```

mac-address-reduction

Enables or disables the MAC address reduction feature.

Syntax

mac-address-reduction [**enable** | **disable**]

Parameters

enable

Enables the MAC address reduction feature.

disable

Disables the MAC address reduction feature.

Modes

Protocol Spanning Tree configuration mode

mac-address-table

Sets the aging time or adds static addresses to the MAC address table, and enables conversational MAC (address) learning.

Syntax

mac-address-table { **aging-time** *seconds* | **conversational** *aging_time* | **learning-mode conversational** }

mac-address-table static *mac-addr* **forward** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **vlan** *vlan_id* }

no mac-address-table

no mac-address-table learning-mode

no mac-address-table static

Command Default

Default aging time is 300 seconds.

Conversational MAC learning is disabled.

Parameters

aging-time *seconds*

Specifies the time in seconds that a learned MAC address will persist after the last update. If the aging time is set to zero (0), it means that aging is disabled. For Brocade VCS Fabric mode, values range from 60 through 100000.

conversational *aging_time*

Configures an aging time for conversational MAC addresses learned by destination address (DA) on an RBridge. If the aging time is set to zero (0), it means that aging is disabled. For Brocade VCS Fabric mode, values range from 60 through 100000.

learning-mode conversational

Enables conversational MAC learning on an RBridge.

static *mac-addr* **forward**

Specifies the Media Access Control (MAC) address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.

forward

Forwards the MAC address to the interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies the port-channel number. Valid values range from 1 through 63.

vlan *vlan_id*
Specifies an active VLAN. Range is from 1 through 4090 if Virtual Fabrics is disabled, and 1 through 8191 if Virtual Fabrics is enabled.

Modes

Global configuration mode

Usage Guidelines

The **vlan** keyword is mandatory because the switch only supports independent VLAN learning (IVL).

Enter **no mac-address-table** to reset the values to their defaults.

Enter **no mac-address-table learning-mode** to disable conversational MAC learning on an RBridge.

Examples

To add the static address 0011.2222.3333 to the MAC address table with a packet received on VLAN 100:

```
switch(config)# mac-address-table static 0011.2222.3333 forward tengigabitethernet 0/1 vlan 100
```

To set the aging time to 10 minutes:

```
switch(config)# mac-address-table aging-time 600
```

To set the aging time to 10 minutes for conversational MAC addresses:

```
switch(config)# mac-address-table aging-time conversational 600
```

To enable conversational MAC learning:

```
switch(config)# mac-address-table learning-mode conversational
```

To disable the static aging time:

```
switch(config)# no mac-address-table aging-time static
```

To disable the conversational aging time:

```
switch(config)# no mac-address-table aging-time conversational
```

To disable static MAC address forwarding on an Ethernet interface:

```
switch(config)# no mac-address-table static aaaa.bbbb.cccc forward tengigabitethernet 1/0/1
```

To disable the aging time by setting its value to 0:

```
switch(config)# mac-address-table aging-time 0
```

Related Commands

show mac-address-table

mac-group

Creates a MAC address group into which one or more end-station MAC addresses are defined, supporting service or transport VFs in a Virtual Fabrics context. The group is used in MAC-based VLAN classification at the access port.

Syntax

mac-group *mac-group-id*

no mac-group *mac-group-id*

Parameters

mac-group-id
A fabric-wide ID. Values range from 1 through 500.

Modes

Global configuration mode

Usage Guidelines

Use this command to enter MAC group configuration mode. In that mode, use the **mac** command to enter one or more MAC addresses that become members of the group.

Enter **no mac-group***mac-group-id* to delete the group and all MAC addresses associated with it.

NOTE
You can add or remove only one MAC address per line.

Examples

To enter MAC group configuration mode and add a MAC address to the group:

```
switch(config)# mac-group 1
switch(config-mac-group 1)# mac abc2.abc2.abc2
```

To remove a MAC address from the MAC group:

```
switch(config-mac-group 1)# no mac abc1.abc2.abc3
```

To remove a MAC group and its associated MAC addresses:

```
switch(config)# no mac-group 1
```

Related Commands

mac, vcs virtual-fabric enable

mac-learning disable vlan

Disables MAC address learning on an interface for specified VLANs.

Syntax

mac-learning disable vlan { **add** | **remove** } { **vlan** *vlan_id* }

no mac-learning disable vlan

Command Default

Dynamic MAC address learning is enabled.

Parameters

add

Adds a VLAN or range of VLANs to the list of VLANs for which dynamic MAC address learning is disabled.

remove

Adds a VLAN or range of VLANs to the list of VLANs for which dynamic MAC address learning is disabled.

vlan*vlan_id*

Specifies a VLAN or range of VLANs. 802.1Q VLANs range from 1 through 4090. Extended VLANs in a Virtual Fabrics context range from 4096 through 8191.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no mac-learning disable vlan** command to enable dynamic MAC address learning for all VLANs on an interface .

Note the following supported configurations and limitations:

- This command is available on all switch ports.
- This command is not available on router ports or virtual routing interfaces. Appropriate error messages will be displayed.
- If this command is configured on a port channel (vLAG), dynamic MAC address learning is disabled on all the member ports. The configuration of this command on the members of the vLAG must be done individually, consistently, and uniformly.
- This command is not available on Inter-Switch Links (ISLs). MAC address learning is always disabled on ISLs. Appropriate error messages will be displayed.
- Source MAC address learning is not supported on VXLAN tunnel interfaces.
- This command is not allowed on a switch port that is attached to a switched virtual interface (SVI). The creation of the SVI will fail if MAC address learning is disabled on any interface that is part of the respective VLAN. Also, ARP resolution is affected if dynamic MAC learning is disabled on a switch port that is associated with a virtual routing interface (SVI).

- This command is disabled for the following VLANs, and appropriate error messages are displayed:
  - 1002 (FCoE VLAN)
  - 4093 (IP over TRILLVLAN)
  - 4095 (control VLAN)
- With CML support, destination MAC address learning is enabled on the switch. Disabling source MAC address learning does not have an effect on destination MAC address learning; however, the same MAC address appearing as a destination MAC address on other ports will trigger flooding.

Examples

To disable dynamic MAC learning on VLAN 10:

```
switch(conf-if-te-4/0/5)# mac-learning disable vlan add 10
```

To disable dynamic MAC learning on VLANs 10 through 20:

```
switch(conf-if-te-4/0/5)# mac-learning disable vlan add 10-20
```

To enable dynamic MAC learning on VLAN 10:

```
switch(conf-if-te-4/0/5)# mac-learning disable vlan remove 10
```

To enable dynamic MAC learning on all VLANs:

```
switch(conf-if-te-4/0/5)# no mac-learning disable
```

History

Release version	Command history
5.0.0	This command was introduced.

mac-rebalance

Forces the rebalancing of EXM entries for the MAC tables.

Syntax

mac-rebalance port-channel *number* { **rbridge-id** *rbridge-id* }

Parameters

port-channel *number*
Specifies the port-channel interface number. Valid values range from 1 through 6144.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Run this command on all remote (non-vLAG) nodes.

To achieve complete utilization of the entire vLAG member links, MAC entries learnt on vLAG need to be equally distributed among the vLAG member nodes. There are some scenarios, in which the EXM entries may not be balanced equally among the vLAG member nodes.

This command is applicable to remote RBridge nodes, such as non-vLAG member nodes. However there are not any restrictions on the usage of this command in vLAG member nodes.

Currently, EXM entries are balanced among the member nodes during RBridge membership changes (add or delete). MACs learned on vLAG are not rebalanced when the link updates (such as during LAG member additions or deletions), to avoid traffic disruption. However, when there are many link updates, the EXM mapping can become unbalanced and eventually overload the link capacity leading to frame drops. The mac-rebalance command corrects this scenario.

In Fabric Cluster mode, RBridge IDs other than the current node's ID are not allowed.

Examples

This example rebalances the EXM entries on RBridge 1 (for vLAG 10):

```
switch# mac-rebalance port-channel 10 rbridge-id 1
```

mac-refresh

Flushes MAC addresses on either the entire cluster or the partner edge loop-detection port.

Syntax

mac-refresh*interval* { **all** | **port** }

no mac-refresh

Command Default

MAC flushing is disabled by default.

Parameters

interval
Specifies the number of seconds between MAC-addresss flushing.

all
Flushes MAC addresses from the entire cluster.

port
Flushes MAC addresses from the partner edge-loop-detection port.

Modes

Edge loop detection mode.

Usage Guidelines

Use the no form of this command to disable MAC-address flushing.

Use this command to remove any MAC inconsistencies in your system. If two interfaces are present in a layer-2 loop, each interface learns the same set of MAC addresses. When ELD detects the layer-2 loop, it puts the participating interface into an operationally down state. Consequently, MAC addresses learned on that interface get flushed. However, the same MAC addresses are present at the interface at the other end of the already detected loop, thereby creating this MAC inconsistency.

To remove this inconsistency, you can run the mac-refresh command to perform a MAC-flush on either the entire cluster or on the partner port at the other end of the loop.

Examples

To flush all MAC addresses in the cluster every 150 seconds:

```
switch# configure
switch (config)# protocol edge-loop-detection
switch (conf-eld)# mac-refresh 150 all
```

History

Release version	Command history
5.0.0	This command was introduced.

management

Enables a variety of Dynamic Host Configuration Protocol (DHCP) management options.

Syntax

management [**interface** { **autoconfig** { **dhcp** | **dhcpv6** }]

no management

Parameters

interface

Enables management options.

autoconfig

Enables automatic configuration of DHCP.

dhcp

Enables DHCP for IPv4.

dhcpv6

Enables DHCP for IPv6.

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no** version of this command to disable this feature.

map fport interface fcoe

Maps VF_Ports to N_Ports in Access Gateway (AG) mode and removes VF_Port to N_Port mapping.

Syntax

map fport interface fcoe *port*

Parameters

port

VF_Port number

Modes

N_Port configuration mode

Usage Guidelines

Use this command to specify a route that AG will use to direct traffic from a device (host or target) on a VF_Port to a fabric switch port connected to an Access Gateway N_Port. The process of specifying routes is called "mapping." Default mapping is enabled for the switch when enabling AG for the first time, You can use the **map** command to change the default mapping.

You must be in the configuration mode for the specific N_Port where you want to map a VF_Port (refer to nport on page 809). N_Ports are designated by the format *rbridge-id/port group/N_Port*, such as 3/0/4 for RBridge 3. Use this format to correctly identify the N_Port in N_Port configuration mode. VF_Ports are identified by the format *domain/rbridge-id/VF_Port*, such as 1/2/26.

Examples

Map VF_Port 1/2/26 to N_Port 2/0/4.

```
sw0(config-rbridge-id-2-ag-nport-if-fi-2/0/4)# map fport interface fcoe 1/2/26
```

Remove map from VF_Port 1/2/26 to N_Port 2/0/4.

```
w0(config-rbridge-id-2-ag-nport-if-fi-2/0/4)# no map fport interface fcoe 1/2/26
```

Related Commands

nport, show ag map

map qos

Adds the QoS profile name as an action to the policy map.

Syntax

map qos *profile_name*

Parameters

profile_name

Designates the name of the QoS profile to be added.

Modes

Policy-map configuration mode

Related Commands

class, policy-map

map sflow

Adds the sFlow profile name as an action to the policy map.

Syntax

map sflow *profile_name*

Parameters

profile_name

Designates the name of the sFlow profile to be added.

Modes

Policy-map configuration mode

Examples

Typical command usage:

```
switch(config)# policy-map p1
switch(config-policymap)# class c1
switch(config-policyclass)# map sflow mysflowmap
```

Related Commands

class, policy-map

map vlan

In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).

Syntax

map vlan [*vlan_id*] {**vni** } [*vni*] [**auto**]

no map vlan *vlan_id*

no map vlan vni

Parameters

vlan_id
A single VLAN ID or range of VLAN IDs. The range is from 1 through 8191. See the Usage Guidelines.

vni
Specifies the VNI (VXLAN Network Identifier) token.

vni
A single VXLAN VNI or range of VXLAN VNIs. The range is from 1 through 16777215. See the Usage Guidelines.

auto
Enables automatic VLAN-to-VNI mapping for every VLAN associated with the tunnel.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Note the following conditions:

- Before using this command, you must first set the VXLAN overlay gateway to layer2-extension, by means of the **type** command.
- Before using this command, you must first configure the appropriate VLANs to be used by the gateway.
- Before mapping VLANs to VNIs manually, you cannot have automatic mapping configured (by means of the **map vlan vni auto** command).
- You cannot map one VLAN to multiple VNIs. Similarly, you cannot map a single VNI to multiple VLANs. For example, vlan to vni mapping should be one to one.
- A single VLAN ID and a range of VLAN IDs can both be specified in a single command as follows: *x,y-z*. The same applies to VNIs.
- When using ranges, you must ensure that the number of values in a VLAN ID range corresponds to the number of values in a VNI range.
- The **no** forms of this command are allowed only if no VLANs are referenced by means of the **extend vlan** command (under a submode of the **site** command). For example, VLANs extended to a site should have a vni mapping.

- The **no map vlan vni auto** command disables the automatic assignment of VNIs. It is not allowed if manual VLAN-to-VNI mappings have been configured. For example, "auto" vlan to vni mapping and "explicit" vlan to vni mapping are mutually exclusive.
- The **no map vlan** *vlan_id* command removes the VNI mappings for one or more VLANs.
- You cannot delete a VLAN (by means of the **no interface vlan** command) that is referenced by means of the **map vlan vni** command.
- This command does not trigger VLAN provisioning, unlike the behavior of the **attach vlan** command.

Examples

To configure a manual mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan 10,20-22 vni 5000-5002,6000
```

This results in the following in the running configuration:

```
overlay-gateway gateway1
  type layer2-extension mode vxlan-ipv4
  map vlan 10 vni 5000
  map vlan 20 vni 5001
  map vlan 21 vni 5002
  map vlan 22 vni 6000
```

To configure an automatic mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan vni auto
```

match

Creates a classification map or "class-map" to classify traffic based on configured match criteria.

Syntax

match *criteria*

Command Default

The only available match criteria at this time is "match any."

Parameters

criteria

Used while in config-classmap mode to configure the match criteria for the class.

Modes

Class-map configuration mode

Usage Guidelines

Use this command to classify traffic based on match criteria. When you launch the **class-map** command, the system is placed in config-classmap mode for the configured map. At this point, you can provide match criteria for the class. The only available match criteria at this time is "match any."

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To configure "match any" match criteria for the class while in config-classmap mode:

```
switch(config-classmap)# match any
```

Related Commands

class-map, show running-config class-map

match (route map)

Defines a variety of match conditions for a route map.

Syntax

match { [**as-path** *name*] | [**community** *acl* **exact-match**] | [**ip address** *acl* | **prefix-list** *string*] | [**ip route-source** *acl* | **prefix** *name*] | [**metric** *num*] | [**next-hop** *address-filter-list*] | [**route-type** [**internal** | **external-type1** | **external-type2**]] | [**level-1** | **level-2** | **level-1-2**] [**tag** *tag-value*] | **interface** *interface interface interface* **. . .** *interface* | [**protocol bgp static-network** | **protocol bgp external** | **protocol bgp internal**] } { **ip address acl** *acl-name* }

no match

no match { **ip address acl** *acl-name* }

Command Default

This option is disabled.

Parameters

as-path

Specifies an AS-path ACL that is configured by the **ip as-path access-list** command.

name

Name of the ACL.

community *acl* **exact-match**

Matches a route if and only if the route community attributes field contains the same community numbers specified in the **match** statement.

ip address

Specifies an IP ACL or prefix list.

acl

ACL that is configured by the **ip as-path access-list** *command.*

prefix-list

Specifies an IP prefix list.

string

Name of the prefix list.

ip route-source

Specifies an IP route source ACL or prefix list.

acl

ACL that is configured by the **ip as-path access-list** *command.*

prefix

IP prefix.

name

Name of the prefix.

metric

Compares the route MED (metric) to the value specified by *num* .

num

BGP4 route metric.

next-hop

Compares the IPv4 address of the route next hop to the specified IP address filters. The filters must be already configured by means of the **distribute-list** command.

address-filter-list

Number of the address filter list configured by means of the **neighbor distribute-list** command.

route-type

Compares a route type to a specified value. Applies to OSPF routes only.

internal

Specifies an internal route.

external-type1

Specifies an External Type 1 route.

external-type2

Specifies an External Type 2 route.

level-1

Compares IS-IS routes only with routes in the same area.

level-2

Compares IS-IS routes only with routes in different areas, but within a domain.

level-1-2

Compares IS-IS routes with routes in the same and in different areas, but within a domain.

tag

Compares the route tag with the specified tag value.

tag-value

Tag value.

interface

Specifies an interface.

interface

Interface type.

protocol bgp static-network

Matches on BGP4 static network routes.

protocol bgp external

Matches on EBGP routes.

protocol bgp internal

Matches on IBGP routes.

ip address acl

Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.

acl-name
The name of the ACL in which matching criteria are specified.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

To match AS-path ACL 1:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# route-map myroutes
switch(config-route-map myroutes)# match as-path 1
```

Related Commands

ip as-path access-list, route-map

match access-list

Configures the access control list to be used with the class map for flow-based QoS.

Syntax

match access-list *acl_name*

Parameters

acl_name

Any valid Layer 2 or Layer 3 ACL access list name.

Modes

Class-map configuration mode

Examples

Example command:

```
switch(config-classmap)#match access-list engineeringACL
```

Related Commands

class-map

match as-path

Matches an AS-path access list name in a route-map instance.

Syntax

match as-path *name*

no match as-path

Parameters

name

Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Related Commands

route-map

match community

Matches a BGP community access list name in a route-map instance.

Syntax

match community *name*

no match community

Parameters

name

Name of a BGP community access list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Related Commands

route-map

match extcommunity

Matches a BGP extended community list in a route-map instance.

Syntax

match extcommunity *number*

no match extcommunity

Command Default

BGP extended community access list names are not matched.

Parameters

name

Extended community list number. Values range from 1 through 99.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no match extcommunity** to remove the community match statement from the configuration file.

Examples

To configure a route map that matches on extended community ACL 1.

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip extcommunity-list 1 permit 123:2
device(config-rbridge-id-122)# route-map extComRmap permit 10
device(config-route-map-extComRmap/permit/10)# match extcommunity 1
```

History

Release version	Command history
5.0.0	This command was introduced.

match interface

Matches interface conditions in a route-map instance.

Syntax

match interface [*<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** | **ve** *rbridge-id/slot/port*]

no match interface

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback

Specifies a loopback port. Values range from 1 through 255.

ve

Specifies a virtual Ethernet port. Range is from 2 through 4090.

rbridge-id

Specifies the RBridge ID.

slot

Specifies the slot number.

port

Specifies the port number.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to configure the interface match clause in a route-map instance. A maximum of three interfaces is supported.

Related Commands

route-map

match ip address

Matches IP address conditions in a route-map instance.

Syntax

match ip address acl *name*

no match ip address acl *name*

Parameters

acl *name*

Name of the access list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IP prefix match clause in a route-map instance.

match ip next-hop

Matches IP next-hop match conditions in a route-map instance.

Syntax

match ip next-hop prefix-list *name*

no match ip next-hop

Parameters

prefix-list *name*

Specifies a prefix list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IP next-hop match clause in a route-map instance.

match ipv6 address

Matches IPv6 address conditions in a route-map instance.

Syntax

match ipv6 address { **prefix-list** *prefix-list-name* }

no match ipv6 address

Command Default

No routes are distributed based on destination network number.

Parameters

prefix-list *prefix-list-name*

Specifies the name of an IPv6 prefix list.

Modes

Route-map configuration mode

Usage Guidelines

Use the no form of this command to disable the BGP graceful restart capability globally for all BGP neighbors.

Use this command to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. .

Examples

To match IPv6 routes that have addresses specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# match ipv6 address prefix-list myprefixlist
```

History

Release version	Command history
5.0.0	This command was introduced.

match metric

Matches a route metric in a route-map instance.

Syntax

match metric *value*

no match metric

Parameters

value

Route metric. Values range from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a route-map metric in route-map instance.

match protocol bgp

Matches BGP routes on protocol types and subtypes in a route-map instance.

Syntax

match protocol bgp [**external** | **internal** | **static-network**]

no match protocol bgp

Parameters

external
Matches EBGP routes.

internal
Matches IBGP routes.

static-network
Matches BGP static routes. This is applicable only for BGP outbound policy.

Modes

Route-map configuration mode

Related Commands

route-map

match route-type

Matches a route type in a route-map instance.

Syntax

match route-type [**internal** | **type-1** | **type-2**]

no match route-type

Parameters

internal
Internal route type

type-1
OSPF external route type 1

type-2
OSPF external route type 2

Modes

Route-map configuration mode

Related Commands

route-map

match tag

Matches a route tag in a route-map instance.

Syntax

match tag *value*

no match tag

Parameters

value

The range of valid values is from 0 through 4294967295.

Modes

Route-map configuration mode

Related Commands

route-map

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

Syntax

max-age *seconds*

no max-age

Command Default

20 seconds.

Parameters

seconds

Configures the Spanning Tree Protocol interface maximum age. Valid values range from 6 through 40.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

Use this command to control the maximum length of time that passes before an interface saves its configuration Bridge Protocol Data Unit (BPDU) information.

If the **VLAN** parameter is not provided, the *seconds* value is applied globally for all per-VLAN instances. However, for VLANs that have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

When configuring the maximum age, the **max-age** command setting must be greater than the **hello-time** command setting. The following relationship should be kept:

```
2*(forward-delay - 1)>=max-age>=2*(hello-time + 1)
```

If xSTP is enabled over VCS, this command must be executed on all RBridges.

Enter **no max-age** to return to the default configuration.

Examples

To configure the maximum-age to 10 seconds:

```
switch(conf-rstp)# max-age 10
```

Related Commands

forward-delay, hello-time

max-hops

Configures the maximum number of hops for a Bridge Protocol Data Unit (BPDU) in an MSTP region.

Syntax

max-hops *hop_count*

no max-hops

Command Default

20 hops

Parameters

hop_count

Specifies the maximum number of hops for which the BPDU will be valid. Valid values range from 1 through 40.

Modes

Protocol Spanning Tree MSTP configuration mode

Usage Guidelines

Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely on the interface. When you change the number of hops, it affects all spanning-tree instances.

Enter **no max-hops** to return to the default value.

Examples

To set the number of maximum hops to 25 for all MSTPs:

```
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# max-hops 25
```

Related Commands

show spanning-tree mst brief

max-mcache

Configures the maximum multicast cache size.

Syntax

max-mcache *num*

no max-mcache

Command Default

Multicast cache size is 2048 entries.

Parameters

num

Number of entries in the multicast cache. Valid values range from 1 through 2048.

Modes

PIM router configuration mode

Usage Guidelines

Enter **no max-mcache** to disable this feature.

Examples

Setting the multicast cache to 500 entries.

```
switch(conf-pim-router)# max-mcache 500
```

max-metric router-lsa

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-vrfs**] [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **ptp** | **stub** | **transit** | **all** } | **on-startup** { *time* | **wait-for-bgp** } [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **ptp** | **stub** | **transit** | **all** }]]

no max-metric router-lsa [**all-vrfs**] [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **ptp** | **stub** | **transit** | **all** } | **on-startup** { *time* | **wait-for-bgp** } [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **ptp** | **stub** | **transit** | **all** }]]

Parameters

all-vrfs
Applies the configuration change to all instances of OSPF.

on-startup
Applies the configuration change at the next OSPF startup.

time
Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86,400.

wait-for-bgp
Indicates that OSPF should wait for either 600 seconds or until BGP has finished route table convergence, whichever happens first, before advertising the links with the normal metric.

summary-lsa *metric-value*
Modifies the metric of all summary type 3 and type 4 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

external-lsa *metric-value*
Modifies the metric of all external type 5 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

all-lsas
Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPF, only the summary-lsa and external-lsa parameters are set.

link
Specifies the types of links for which the maximum metric is advertised. By default, the maximum metric is advertised only for transit links.

all
Advertises the maximum metric in Router LSAs for all supported link types.

ptp
Advertises the maximum metric in Router LSAs for point-to-point links.

stub
Advertises the maximum metric in Router LSAs for stub links.

transit

Advertises the maximum metric in Router LSAs for transit links. This is the default link type.

Modes

OSPF VRF router configuration mode

Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa all-lsas** to disable advertising the maximum metric value in different LSAs.

Examples

To advertise the maximum metric value using the **all-lsas** option:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# max-metric router-lsa all-lsas
```

max-route

Sets the maximum number of routes for VRF.

Syntax

max-route *value*

Parameters

value

The maximum number of routes.

Modes

VRF configuration mode

Related Commands

vrf

maxas-limit

Imposes a limit on the number of autonomous systems in the AS-PATH attribute.

Syntax

maxas-limit { **in** } *num*

no maxas-limit { **in** } *num*

Command Default

This option is disabled.

Parameters

in

Allows an AS-PATH attribute from any neighbor imposing a limit on the number of autonomous systems.

num

Valid range is from 0 through 300.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

The following example sets the limit on the number of autonomous systems in the AS-PATH attribute to 100.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# maxas-limit 100
```

maximum-paths (BGP)

Changes the maximum number of BGP4 and BGP4+ shared paths.

Syntax

maximum-paths *num* | **use-load-sharing**

no maximum-paths

Command Default

This option is disabled.

Parameters

num

Maximum number of paths across which the device balances traffic to a given BGP4 destination. Valid values range from 2 through 8. The default is 1.

use-load-sharing

Uses the maximum IP ECMP path value that is configured by means of the **ip load-sharing** command.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the value configured by the **ip load-sharing** command.

Use the **no** form of this command to restore the default.

Examples

The following example sets the maximum number of BGP4 shared paths to 8.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# maximum-paths 8
```

The following example sets the maximum number of BGP4+ shared paths to that of the value already configured using the **ip load-sharing** command.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv6 unicast
switch(config-bgp-ipv6u)# maximum-paths use-load-sharing
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

maximum-paths ebgp ibgp (BGP)

maximum-paths ebgp ibgp (BGP)

Specifies the number of equal-cost multipath EBGP or IBGP routes or paths that are selected.

Syntax

maximum-paths { **ebgp** *num* | **ibgp** *num* }

no maximum-paths

Command Default

This option is disabled.

Parameters

ebgp

Specifies EBGP routes or paths.

ibgp

Specifies IBGP routes or paths.

num

The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 8. 1 disables equal-cost multipath.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Enhancements to BGP4 load sharing support the load sharing of BGP4 and BGP4+ routes in IP Equal-Cost Multipath (ECMP, even if the BGP4 multipath load-sharing feature is not enabled by means of the **use-load-sharing** option to the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath EBGP or IBGP routes or paths that are selected.

Use the **no** form of this command to restore the default.

Examples

The following example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 6.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# maximum-paths ebgp 6
```

The following example sets the number of equal-cost multipath IBGP routes or paths that will be selected to 4.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv6 unicast
switch(config-bgp-ipv6u)# maximum-paths ibgp 4
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

med-missing-as-worst

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Syntax

med-missing-as-worst

no med-missing-as-worst

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs. Use this command to configure the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Use the **no** form of this command to restore the default.

Examples

Typical example of this command:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# med-missing-as-worst
```

message-interval

Configures the Protocol Independent Multicast (PIM) Join/Prune message interval.

Syntax

message-interval *num*

no message-interval

Command Default

60 seconds

Parameters

num

The interval value in seconds. Valid values range from 10 through 65535 seconds.

Modes

PIM router configuration mode

Usage Guidelines

Use this command to specify the interval at which the periodic PIM Join/Prune messages must be sent out.

Enter **no message-interval** to disable this feature.

Examples

Setting the interval to one hour.

```
switch(conf-pim-router)# message-interval 3600
```

Related Commands

router pim

metric-type

Configures the default metric type for external routes.

Syntax

metric-type { **type1** | **type2** }

no metric-type { **type1** | **type2** }

Command Default

type1

Parameters

type1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

type2

The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Modes

OSPF/OSPFv3 VRF router configuration mode

Usage Guidelines

The **no** form of this command returns to the default setting. You must specify a type parameter when usiing the **no** form.

Examples

To set the default metric type for external routes to type2:

```
device# configure terminal
device(config)# rbridge-id 5
device(config-rbridge-id-5)# router ospf
device(config-router-ospf-vrf-default-vrf)# metric-type type2
```

History

Release version	Command history
5.0.0	Support was added for OSPFv3.

Related Commands

default-information-originate (OSPF)

minimum-links

Sets the minimum bandwidth.

Syntax

minimum-links *num-of-links*

no minimum-links

Command Default

Number of links is 1.

Parameters

num-of-links

Number of links. Valid values range from 1 through 32.

Modes

Port-channel interface configuration mode

Usage Guidelines

Use this command to allow a port-channel to operate at a certain minimum bandwidth all the time. If the bandwidth of the port-channel drops below that minimum number, then the port-channel is declared operationally DOWN even though it has operationally UP members.

Enter **no minimum-links** to restore the default value.

Examples

To set the minimum number of links to 16 on a specific port-channel interface:

```
switch(config)# interface port-channel 33

switch(config-port-channel-33)# minimum-links 16
```

mode

Sets the LLDP mode on the switch.

Syntax

mode { **tx** | **rx** }

Command Default

Both transmit and receive modes are enabled.

Parameters

tx

Specifies to enable only the transmit mode.

rx

Specifies to enable only the receive mode.

Modes

Protocol LLDP configuration mode

Examples

To enable only the transmit mode:

```
switch(conf-lldp)# mode tx
```

To enable only the receive mode:

```
switch(conf-lldp)# mode rx
```

Related Commands

show lldp interface

mode (27x40 GbE line card)

Sets Performance or Density operating modes on the 27x40 GbE line card installed in the 8770 Switch.

Syntax

mode performance

no mode performance

Command Default

Density mode (**no mode performance**) is enabled.

Modes

port-group

Usage Guidelines

Use this command to set Performance or Density (default) operating modes for port groups 1-9 on the 27x40 GbE line card. When a port group is configured In Performance mode, the third port in the port group is persistently disabled, but the remaining two ports operate at up to 40 Gbps in Performance mode to achieve the 80 Gbps maximum rate for the port group. QSFP breakout mode is only supported on ports configured in Performance mode.

If Density mode (default) is configured for a port group, all three ports in the group are enabled in Density mode, so cannot support the 40 Gbps maximum rate. If this mode is configured on all port groups, 27 total ports are available for use.

For more information on port groups and the Performance and Density operating modes on the line card, refer to the "Overview" chapter in the Brocade 8770-4 and 8770-8 Hardware Reference Manuals.

Enter **no performance mode** to restore the default value. Power off the line card before configuring operating modes.

Examples

To enable Performance mode on port group 9 of the line card in slot 3 of switch with RBridge ID 1.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# hardware
switch(config-hardware)# port-group 1/3/9
switch(config-port-group-1/3/9)# mode performance
%Warning: port-group mode performance is a disruptive command.
Please save the running-config to startup-config and a power-cycle for the
changes to take place.
```

Related Commands

hardware, port-group

modes

Enables and disables operating modes for port groups for Access Gateway mode.

Syntax

modes *mode_name*

no modes *mode_name*

Command Default

lb

Parameters

mode_name

lb (Automatic Login Balancing)

Modes

Port Grouping configuration mode

Usage Guidelines

Login Balancing (LB) is the only mode that you can enable. Automatic Login Balancing is enabled by default for a port group when the port group is created. If LB mode is enabled for a port group and a VF_Port goes offline, logins in the port group are redistributed among the remaining VF_Ports. Similarly, if an N_Port comes online, port logins in the port group are redistributed to maintain a balanced N_Port-to-VF_Port ratio.

You must be in Port Grouping configuration mode for a specific port group to use this command. Entering **no modes** *mode_name* disables the mode.

Consider the following when using LB mode with **show running-config ag** and **show ag** commands:

- The only Port Grouping mode that you can enable or disable is LB mode.
- When LB mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the configured VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, **show ag**, and **show ag map** displays the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples

Enable Automatic Login Balancing mode on port group 8.

```
sw0(config-rbridge-id-3-ag-pg-8)# modes lb
```

Disable Automatic Login Balancing mode on port group 8.

```
sw0(config-rbridge-id-3-ag-pg-8)# no modes lb
```

monitor session

Enables a Port Mirroring session for monitoring traffic.

Syntax

monitor session *session_number*

no monitor session *session_number*

Parameters

session_number
Specifies a session identification number. Valid values range from 1 through 512.

Modes

Global configuration mode

Usage Guidelines

Enter **no monitor session** to delete the port mirroring session.

Examples

To enable session 22 for monitoring traffic:

```
switch# configure
switch(config)# monitor session 22
```

Related Commands

source

monitor session (VXLAN)

Enables switched port analyzer (SPAN) on one or all tunnels of a VXLAN overlay gateway.

Syntax

monitor session *session_number* **direction** { **tx** | **rx** | **both** } [**remote-endpoint** { *ip_address* | **any** }] **vlan** [**add** | **remove**] *VLAN_ID_range*

no monitor session *session_number*

Parameters

session_number
Specifies the SPAN session ID that was configured with the global **monitor session** command.

tx
Enables SPAN for the transmitting tunnels.

rx
Enables SPAN for the receiving tunnels.

both
Enables SPAN for both the transmitting and receiving tunnels.

ip_address
Enables SPAN for the specified the IPv4 address of the remote Hypervisorfor the NSX Controller to VXLAN termination endpoint (VTEP).

any
Enables SPAN for all tunnels on the gateway.

add
Enables SPAN on specified VLAN IDs. You can use this option if you have disabled SPAN on specific VLAN IDs and now want to re-enable SPAN on these IDs.

remove
Disables SPAN on specified VLAN IDs.

VLAN_ID_range
Specifies the VLAN IDs for enabling SPAN.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Use this command to enable SPAN on one or all tunnels of this gateway for specified VLANs. You can use the **remote-endpoint** option to choose all tunnels or specific tunnels of this gateway. You choose a specific tunnel by specifying the remote Hypervisor 's VTEP IP address. This address is matched with the destination IP address of the tunnels.

The **remove** option can be used to exclude VLANs from a previously configured list. If all the VLANs are removed, the entire SPAN configuration is deleted (this is the same behavior as thatresulting from the **no monitor session** *session_number* command).

The only way to change the direction once you have run this command is to remove the SPAN configuration, then rerun the **monitor session** command. Specified VLANs must already be configured as exported through this gateway.

The SPAN session number must already be configured, and the SPAN destination must already be specified and cannot be a tunnel.

The SPAN session must not include source port configuration for this gateway.

The deletion of an attached VLAN (by using the **no attach vlan** command) is blocked if SPAN has been enabled for the VLAN you are trying to delete.

The **no** form of this command removes SPAN configuration for the gateway.

Examples

To enable SPAN for all tunnels in both directions for"gateway1" on VLAN IDs 1 through 10 and SPAN session ID 3:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# monitor session 3 direction both remote-endpoint any vlan add 1-10
```

Related Commands

overlay-gateway

mtu

Specifies the size of the maximum transmission unit (MTU) on an interface.

Syntax

mtu *size*

Command Default

Interfaces have a default MTU of 2500 bytes.

Parameters

size

Size, in bytes, of the MTU. Range is from 1522 through 9216.

Modes

Interface subtype configuration mode

Usage Guidelines

Configuring an MTU on a VLAN interface is not valid.

If you use the **ipv6 mtu** command to change the MTU value for IPv6 functionality, you must set the same value on the interface by using the **mtu** command. Otherwise packets will be dropped.

The only MTU size available on a VXLAN is 9156 bytes, due to hardware restrictions.

multipath (BGP)

Changes load sharing to apply to only IBGP or EBGP paths, or to support load sharing among paths from different neighboring autonomous systems (ASs).

Syntax

multipath [**ebgp** | **ibgp** | **multi-as**]

no multipath

Command Default

This option is disabled.

Parameters

ebgp
Enables load sharing of EBGP paths only.

ibgp
Enables load sharing of IBGP paths only.

multi-as
Enables load sharing of paths from different neighboring autonomous systems.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

By default, when BGP4 load sharing is enabled, both IBGP and EBGP paths are eligible for load sharing, while paths from different neighboring autonomous systems are not. Use this command to change load sharing to apply to only IBGP or EBGP paths, or to support load sharing among paths from different neighboring autonomous systems.

Use the **no** form of this command to restore the default.

Examples

To change load sharing to apply to IBGP paths:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# multipath ibgp
```

To enable load sharing of paths from different neighboring autonomous systems:

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# router bgp
switch(config-bgp-router)# address-family ipv6 unicast
switch(config-bgp-ipv6u)# multipath multi-as
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

multiplier (LLDP)

Sets the number of consecutive misses of hello messages before LLDP declares the neighbor as dead.

Syntax

multiplier *value*

no multiplier

Command Default

Multiplier default value is 4.

Parameters

value

Specifies a multiplier value to use. Valid values range from 2 through 10.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no multiplier** to return to the default setting.

Examples

To set the number of consecutive misses:

```
switch(conf-lldp)# multiplier 2
```

Related Commands

hello-interval (ELD)

multiplier (UDLD)

Sets timeout multiplier for missed UDLD PDUs.

Syntax

multiplier *value*

no multiplier

Command Default

Multiplier default value is 5.

Parameters

value

Specifies a multiplier value to use. Valid values range from 3 through 10.

Modes

Protocol UDLD configuration mode

Usage Guidelines

When the device at one end is a Brocade IP product, the timeout interval is the product of the "hello" time interval at the other end and the "multiplier" value.

When the UDLD protocol times out waiting for UDLD PDUs, it will block the port.

Enter **no multiplier** to return to the default setting.

Examples

To set the multiplier to 8:

```
switch(config)# protocol udld
switch(config-udld)# multiplier 8
```

Related Commands

hello (UDLD)

name (VLAN interfaces)

Assigns a descriptive name to a VLAN. Although this name cannot be used in place of the *vlan_ID*, it is displayed in response to the **show vlan brief** command.

Syntax

name *vlan_name*

no name

Parameters

vlan_name
Specifies the characters of the name. The string must be between 1 and 32 characters.

Modes

VLAN interface sub-type

Usage Guidelines

If no name is assigned to a VLAN, a default name is automatically assigned, composed of "VLAN" and the *vlan_ID*. For example, if the *vlan_ID* is 1000, the default name is VLAN1000.

To revert from an assigned name to the default name, enter **no name**.

Examples

Assign the name "marketing" to VLAN 1000:

```
device# configure
device(config)# interface vlan 1000
device(config-Vlan-1000)# name marketing
device(config-Vlan-1000)
```

History

Release version	Command history
5.0.1	This command was introduced.

Related Commands

show vlan brief

nas auto-qos

Enables the Quality of Service (QoS) functionality for the Auto-NAS (automatic network attached storage) feature.

Syntax

nas auto-qos

no nas auto-qos

Modes

Global configuration mode

Usage Guidelines

This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Use the **no** form of this command to disable the Auto-NAS feature.

nas server-ip

Identifies the port that is to receive Auto NAS (automatic network attached storage) traffic.

Syntax

nas server-ip *address/prefix* [**vlan** *vlan_ID* | **vrf** *vrf_name*]

no nas server-ip *address*

Parameters

address/prefix
IP address/prefix to receive NAS traffic.

vlan *vlan_ID*
VLAN ID.

vrf *vrf_name*
VRF name.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Use the **no** form of this command to remove a nas server-ip prefix.

Examples

To identify an IP address/prefix of 2.2.2.2/32 to receive NAS traffic over VLAN 10:

```
switch# configure
switch(config)# nas server-ip 2.2.2.2/32 vlan 10
```

nbr-timeout

Configures the neighbor timeout interval after which a neighbor is considered to be absent.

Syntax

nbr-timeout *num*

no nbr-timeout

Command Default

The default is 105.

Parameters

num

Interval value in seconds. Valid values range from 35 through 12600 seconds.

Modes

PIM router configuration mode

Usage Guidelines

Enter **no nbr-timeout** to disable this feature.

Examples

Setting the timeout to 600 seconds.

```
switch(conf-pim-router)# nbr-timeout 600
```

Related Commands

router pim

neighbor (BGP)

Assigns a neighbor to a specified IPv4 address or peer group to provide a variety of configuration options.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } { **advertisement-interval** | **as-override** | **capability** | **description** | **ebgp-multihop** | **enforce-first-as** | **local-as** | **maxas-limit** | **next-hop-self** | **password** | **peer-group** | **remote-as** | **remove-private-as** | **shutdown** | **soft-reconfiguration** | **static-network-edge** | **timers** | **update-source** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } { **advertisement-interval** | **as-override** | **capability** | **description** | **ebgp-multihop** | **enforce-first-as** | **local-as** | **maxas-limit** | **next-hop-self** | **password** | **peer-group** | **remote-as** | **remove-private-as** | **shutdown** | **soft-reconfiguration** | **static-network-edge** | **timers** | **update-source** }

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Alphanumeric characters. Range is from 1 through 63.

advertisement-interval
See **neighbor advertisement-interval (BGP)**.

as-override
See **neighbor as-override (BGP)**.

capability
See **neighbor capability as4 (BGP)**.

description
See **neighbor description (BGP)**.

ebgp-multihop
See **neighbor ebgp-multihop (BGP)**.

enforce-first-as
See **neighbor enforce-first-as (BGP)**.

local-as
See **neighbor local-as (BGP)**.

maxas-limit
See **neighbor maxas-limit in (BGP)**.

next-hop-self
See **neighbor next-hop-self (BGP)**.

password
See **neighbor password (BGP)**.

peer-group
See **neighbor peer-group (BGP)**.

remote-as
See **neighbor remote-as (BGP)**.

remote-private-as
See **neighbor remove-private-as (BGP)**.

shutdown
See **neighbor shutdown (BGP)**.

soft-reconfiguration
See **neighbor soft-reconfiguration inbound (BGP)**.

static-network-edge
See **neighbor static-network-edge (BGP)**.

timers
See **neighbor timers (BGP)**.

update-source
See **neighbor update-source (BGP)**.

Modes

BGP configuration mode

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Neighbor configuration appears in both BGP global and BGP Address-Family command modes. The neighbor parameters/attributes that are common to all of the address families appear in the global mode, making support available for IPv6 address families in the future. The neighbor parameters/attributes that are specific to the address-family appear within the address-family submode.

Use the **no** form of this command to remove the neighbor from the specified peer group or remove an option.

Examples

To assign a neighbor to a specified peer group and view available options:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13  ?
Possible completions:
  advertisement-interval   Minimum interval between sending BGP routing updates
  as-override              Override matching AS-number while sending update
  capability               Advertise capability to the peer
  description              Neighbor by description
  ebgp-multihop            Allow EBGP neighbors not on directly connected
                           networks
  enforce-first-as         Enforce the first AS for EBGP routes
  local-as                 Assign local-as number to neighbor
  maxas-limit              Impose limit on number of ASes in AS-PATH attribute
  next-hop-self            Disable the next hop calculation for this neighbor
  password                 Enable TCP-MD5 password protection
  peer-group               Create Peer Group
  remote-as                Specify a BGP neighbor
  remove-private-as        Remove private AS number from outbound updates
  shutdown                 Administratively shut down this neighbor
  soft-reconfiguration     Per neighbor soft reconfiguration
  timers                   BGP per neighbor timers
  update-source            Source of routing updates
```

To assign a neighbor to a specified peer group in BGP address-family IPv6 unicast configuration mode and view available options:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:700:122:57::57 ?
Possible completions:
  activate                 Allow exchange of route in the current family mode
  allowas-in               Disables the AS_PATH check of the routes learned
                           from the AS
  capability               Advertise capability to the peer
  default-originate        Originate default route to peer
  filter-list              Establish BGP filters
  maximum-prefix           Maximum number of prefix accept from this peer
  prefix-list              Prefix List for filtering routes
  route-map                Apply route map to neighbor
  route-reflector-client   Configure a neighbor as Route Reflector client
  send-community           Send community attribute to this neighbor
  unsuppress-map           Route-map to selectively unsuppress suppressed
                           routes
  weight                   Set default weight for routes from this neighbor
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

neighbor (OSPF)

Manually configures a neighbor.

Syntax

neighbor *A.B.C.D*

no neighbor

Command Default

Neighbors are not configured.

Parameters

A.B.C.D

IPv4 address of the neighbor.

Modes

OSPF VRF router configuration mode

Usage Guidelines

This command is typically used in point-to-point networks.

OSPF Hellos must use a unicast address, not broadcast or multicast packets.

Enter **no neighbor***A.B.C.D* to remove the specified neighbor.

Examples

To configure a neighbor whose IPv4 address is 1.1.1.1:

```
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# neighbor 1.1.1.1
```

neighbor activate

Enables the exchange of information with BGP neighbors and peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

Command Default

Disabled.

Parameters

ip-address
Specifies the IPv4 address of the neighbor

ipv6-address
Specifies the IPv6 address of the neighbor

peer-group-name
Specifies a peer group.

Modes

BGP address-family IPv4 unicast configuration mode.

BGP address-family IPv6 unicast configuration mode.

Usage Guidelines

Use the **no** form of this command to disable the exchange of an address with a BGP neighbor or peer group.

Examples

To establish a BGP session with a BGP neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 neighbor activate
```

History

Release version	Command history
5.0.0	This command was introduced.

neighbor advertisement-interval

Enables changes to interval over which a specified neighbor or peer-group holds route updates before forwarding them.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval** *seconds*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval** *seconds*

Command Default

The default is 0.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

seconds
Range is from 0 through 3600.

Modes

BGP configuration mode

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 advertisement-interval 60
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor allowas-in

Disables the AS_PATH check function for routes learned from a specified location so that BGP does not reject routes that contain the recipient BGP speaker's AS number.

Syntax

neighbor {*ip-address* | *ipv6-address* | *peer-group-name* } **neighbor allowas-in** *number*

no neighbor allowas-in {*ip-address* | *ipv6-address* | *peer-group-name* } **neighbor allowas-in** *number*

Command Default

The AS_PATH check function is enabled and any route whose path contains the speaker's AS number is rejected as a loop.

Parameters

ip-address
: Specifies the IP address of the neighbor

ipv6-address
: Specifies the IPv6 address of the neighbor

peer-group-name
: Specifies a peer group.

number
: Specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted. Valid values are one through ten.

Modes

BGP address-family IPv4 unicast configuration mode.

BGP address-family IPv6 unicast configuration mode.

Usage Guidelines

Use the **no** form of this command to re-enable the AS_PATH check function.

Examples

To specify that the AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted.

```
device#configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 allowas-in 3
```

History

Release version	Command history
5.0.0	This command was introduced.

neighbor as-override

Replaces the autonomous system number (ASN) of the originating router with the ASN of the sending BGP router.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

Usage Guidelines

Use this command to replace the ASN of the originating router with the ASN of the sending BGP router.

BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

Use the **no** form of this command to disable this feature.

Examples

To change an advertisement interval:

```
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor capability as4

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**enable** | **disable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**enable** | **disable**]

Command Default

Four-byte ASNs are disabled by default.

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

enable
: Enables 4-byte numbering.

disable
: Disables 4-byte numbering.

Modes

BGP configuration mode

Usage Guidelines

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for AS4.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor capability orf prefixlist

Advertises outbound route filter (ORF) capabilities to peer routers.

Syntax

neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

no neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

Command Default

ORF capabilities are not advertised to a peer router.

Parameters

ip_address
: Specifies the IPv4 address of the neighbor

ipv6_address
: Specifies the IPv6 address of the neighbor

peer-group-name
: Specifies a peer group.

receive
: Enables the ORF prefix list capability in receive mode.

send
: Enables the ORF prefix list capability in send mode.

Modes

BGP address-family IPv4 unicast configuration mode.

BGP address-family IPv6 unicast configuration mode.

Usage Guidelines

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Use the **no** form of this command to disable ORF capabilities.

Examples

To advertise the ORF send capability to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 capability orf prefixlist send
```

To advertise the ORF receive capability to a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 capability orf prefixlist receive
```

History

Release version	Command history
5.0.0	This command was introduced.

neighbor default-originate

Configures the device to send the default route 0.0.0.0 to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-name*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-name*]

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

route-map
Optionally injects the default route conditionally, depending on the match conditions in the route map.

map-name
Name of the route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 default-originate route-map  myroutemap
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

neighbor description

Specifies a name for a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description** *string*

no neighbor { *ip-address* | *peer-group-name* } **description** *string*

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

description *string*
Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the name.

Examples

```
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 description mygoodneighbor
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor ebgp-multihop

Allows EBGP neighbors that are not on directly connected networks and sets an optional maximum hop count.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multiphop** [*max-hop-count*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multiphop** [*max-hop-count*]

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

max-hop-count
Maximum hop count (optional). Range is from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this feature.

Examples

```
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 ebgp-multihop 20
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor enforce-first-as

Ensures that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**enable** | **disable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**enable** | **disable**]

Command Default

This feature is disabled: A device does not require the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

enable
Enables this feature.

disable
Disables this feature.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this requirement globally for the device.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor filter-list

Specifies a filter list to be applied to updates from or to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

ip-prefix-list-name
Name of the filter list.

in
Specifies that the list is applied on updates received from the neighbor.

out
Specifies that the list is applied on updates sent to the neighbor.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 filter-list myfilterlist out
```

To specify that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 filter-list 2 in
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

neighbor local-as

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an EBGP peer.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Local ASN. Range is from 1 through 4294967295.

no-prepend
Causes the device to stop pre-pending the selected ASN.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the local ASN.

Examples

To ensure that a device prepends the local ASN:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

To stop the device from pre-pending the selected ASN:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor maxas-limit in

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in** { *num* | **disable** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in** { *num* | **disable** }

Command Default

Disabled.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Maximum length of the AS path. Range is from 0 through 300. The default is 300.

disable
Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration at the global level.

Examples

To change the length of the maximum allowed AS path length from the default:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```

To prevent a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 maxas-limit in disable
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor maximum-prefix

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Maximum number of IP prefixes that can be learned. Range is from 0 through 4294967295. Default is 0 (unlimited).

threshold
: Specifies the percentage of the value specified by *num* that causes a syslog message to be generated. Range is from 1 through 100. Default is 100.

teardown
: Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 maximum-prefix 100000 threshold 80
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

neighbor next-hop-self

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

always
Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration at the global level.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 next-hop-self
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor password

Specifies an MD5 password for securing sessions between the device and a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password** *string*

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Alphanumeric characters. Range is from 1 through 63.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration at the global level.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 password s0M3P@55W0Rd
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor peer-group

Enables the creation of a BGP peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **peer-group** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **peer-group** *string*

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Alphanumeric characters. Range is from 1 through 63.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the peer group.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 peer-group mypeergroup1
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor prefix-list

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Name of the prefix list.

in
Applies the filter in incoming routes.

out
Applies the filter in outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

To apply the prefix list myprefixlist to outgoing advertisements to neighbor 2001:2018:8192::125.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

neighbor remote-as

Specifies the autonomous system (AS) in which a remote neighbor resides.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as** *num*

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

num
Remote AS number (ASN). Range is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the neighbor from the AS.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remote-as 100
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor remove-private-as

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

Usage Guidelines

The device will remove ASNs 64512 through 65535 (the well-known BGP4 private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

Use the **no** form of this command to restore the default.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remove-private-as
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor route-map

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes defined in a route map.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

in
Applies the filter on incoming routes.

string
Name of the route map.

out
Applies the filter on outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-map myroutemap out
```

To apply a route map named myroutemap to a BGP incoming route from 2001:2018:8192::125

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 route-map myroutemap in
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

neighbor route-reflector-client

Configures a neighbor to be a route-reflector client.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

Use the **no** form of this command to restore the default.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-reflector-client
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

neighbor send-community

Enables sending the community attribute in updates to the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

Command Default

The device does not send community attributes.

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

both
Sends both standard and extended attributes.

extended
Sends extended attributes.

standard
Sends standard attributes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 send-community standard
```

To send extended communities attributes to a BGP neighbor at IPv6 address 2001:2018:8192::125.

```
device# configure terminal
ddevice(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 send-community extended
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

neighbor shutdown

Causes a device to shut down the session administratively with its neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** { **generate-rib-out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** { **generate-rib-out** }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

generate-rib-out
: When a peer is put into shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

Modes

BGP configuration mode

Usage Guidelines

Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

Use the **no** form of this command to restore the defaults.

Examples

To cause a device to shut down the session administratively with its neighbor:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

To cause a device to shut down the session administratively with its neighbor and generate RIB outbound routes:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 shutdown generate-rib-out
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor soft-reconfiguration inbound

Stores all the route updates received from a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

Usage Guidelines

Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 or BGP4+ route table or resetting the session with the neighbor.

Use the **no** form of the command to disable this feature.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 soft-configuration inbound
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor timers

Specifies how frequently a device sends KEEPALIVE messages to its BGP neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *value* **hold-time** *value*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *value* **hold-time** *value*

Command Default

Refer to the Parameters section for specific defaults.

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

value
: Keep-alive timer. Range is from 0 through 65535 seconds. The default is 60.

value
: Hold timer. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor unsuppress-map

Removes route suppression from neighbor routes when those routes have been suppressed as a result of aggregation. All routes matching route-map rules are unsuppressed.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

string
Name of the route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 unsuppress-map myroutemap
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

neighbor update-source

Configures the device to communicate with a neighbor through a specified interface.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | *<N>* **gigabitethernet** | **loopback** *num* | **ve-interface** *vlan_id* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | *<N>* **gigabitethernet** | **loopback** *num* | **ve-interface** *vlan_id* }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

ip-address
: IP address of the update source.

*<N>***gigabitethernet**
: Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

  rbridge-id
  : Specifies an RBridge ID.

  slot
  : Specifies a valid slot number.

  port
  : Specifies a valid port number.

loopback *num*
: Specifies a loopback interface.

ve-interface *vlan_id*
: Specifies a virtual Ethernet VLAN interface.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

```
device#configure terminal
device#(config)# rbridge-id 10
device#(config-rbridge-id-10)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 update-source tengigabitethernet 15/1/1
```

History

Release version	Command history
5.0.0	This command was modified to add support for IPv6.

neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

Command Default

The default for *num* is 0.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor

peer-group-name
Name of the peer group.

num
Value from 1 through 65535.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

BGP4 prefers larger weights over smaller weights.

Use the **no** form of the command to restore the defaults.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 weight 100
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

network (BGP)

Configures the device to advertise a network.

Syntax

network *network/mask* [**route-map** *map-name*] | [**weight** *num*] | [**backdoor**]

no network *network/mask* [**route-map** *map-name*] | [**weight** *num*] | [**backdoor**]

Command Default

No network is advertised.

Parameters

network/mask
Network and mask in CIDR notation.

map-name
Name of the route map with which to set or change BGP4 attributes for the network to be advertised.

num
Weight to be added to routes to this network. Range is 0 through 65535. The default is 0.

backdoor
Changes administrative distance of the route to this network from the EBGP administrative distance (the default is 20) to the local BGP4 weight (the default is 200), tagging the route as a backdoor route.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

BGP4 prefers larger weights over smaller weights.

Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# network 10.11.12.13/30 route-map myroutemap
```

To import the IPv6 prefix 2001:db8::/32 into the BGP4+ database and set a weight of 300:

```
switch# config
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# address-family ipv6 unicast
switch(config-bgp-ipv4u)# network 2001:db8::/32 weight 300
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

next-hop-enable-default

Configures the device to use the default route as the next hop.

Syntax

next-hop-enable-default

no next-hop-enable-default

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-enable-default
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

next-hop-recursion

Enables recursive next-hop lookups.

Syntax

next-hop-recursion

no next-hop-recursion

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

If the BGP next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

Use the **no** form of this command to restore the default.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-recursion
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

nonstop-routing

Enables nonstop-routing (NSR) for OSPFv3.

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Use the **no** form of this command to disable non-stop routing.

Examples

To enable NSR on a device:

```
switch# config
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 router ospf
switch(config-ipv6-router-ospf-vrf-default-vrf)# nonstop-routing
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

graceful-restart helper (OSPFv3)

nport

Enables N_Port configuration mode for a specific N_Port ID for Access Gateway mode.

Syntax

nport *port*

no nport *port*

Parameters

port

N_Port number supported by hardware platform.

Modes

Access Gateway (AG) configuration

Usage Guidelines

This command enables N_Port configuration mode for a specific N_Port number so that you can map VF_Ports to the N_Port (Port Mapping).

To use this command, you must be in Access Gateway (AG) configuration mode, This command enables N_Port configuration mode for the specific N_Port. While in this mode, you can map VF_Ports to the N_Port. Enter the N_Port in RBridge ID/port group ID/N_Port ID format, such as 3/0/4 for Rbridge 3, port group 0 (default port group), and N_Port 4.

Examples

Enabling N_Port configuration mode for N_Port 4 while in AG configuration mode.

```
sw0(config-rbridge-id-2-ag)# nport 2/0/4
sw0(config-rbridge-id-2-ag-nport-if-fi-2/0/4)#
```

Related Commands

map fport interface fcoe, show ag

nport interface Fibrechannel

Adds or deletes N_Ports in a specified port group for Access Gateway mode.

Syntax

nport interface Fibrechannel *port*

no nport interface Fibrechannel *port*

Parameters

port

N_Port number supported by switch model.

Modes

Port Grouping configuration mode

Usage Guidelines

To use this command, you must be in Port Grouping configuration mode for a specific port group. Before adding an N_Port to a port group, you must remove the N_Port from its current port group unless the port resides in default port group 0 (pg 0). N_Ports are identified by the format *rbridge-id/slot/N_Port*, such as 3/0/4 for RBridge 3, slot 0, and N_Port 4.

Examples

Adding N_Port 3/0/3 to port group 2 (pg 2):

```
sw0(config-rbridge-id-3-ag-pg-2)# nport interface Fibrechannel 3/0/3
```

Removing N_Port 3/0/3 from port group 3 (pg 3)

```
sw0(config-rbridge-id-3-ag-pg-3)# nport interface Fibrechannel 3/0/3
```

Related Commands

pg, show ag pg

nssa-translator

Configures Not So Stubby Area (NSSA) Type 7-to-Type 5 Link State Advertisement (LSA) translation.

Syntax

nssa-translator

no nssa-translator

Modes

OSPF VRF router configuration mode

Usage Guidelines

Use this command to enable or disable NSSA Type 7-to-Type 5 LSA translation on the NSSA Area Border Router (ABR). Translation may be needed if routers within the NSSA need to know about external routes. However, disabling this translation can be useful when the router is an area border router with many NSSA areas, and does not need to export the NSSA external routes into the backbone

Enter **no nssa-translator** to disable NSSA Type 7-to-Type 5 translation.

Examples

To disable NSAA Type 7-to-Type 5 LSA translation:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# no nssa-translator
```

nsx-controller client-cert

Generates or deletes a self-signed certificate for the VXLAN gateway.

Syntax

nsx-controller client-cert { **generate** | **delete** }

Parameters

generate

Generates a self-signed certificate for the VXLAN gateway.

delete

Deletes the certificate.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported in logical chassis cluster mode only.

Examples

To generate a self-signed certificate for the VXLAN gateway:

```
switch# nsx-controller client-cert generate
```

nsx-controller name

Creates an NSX controller connection profile or enters NSX controller configuration mode for an existing NSX controller connection profile.

Syntax

nsx-controller *name*

no nsx-controller *name*

Parameters

name

Specifies a name for the NSX controller. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Modes

Global configuration mode

Usage Guidelines

Only one NSX Controller connection profile can be configured.

This command is supported in logical chassis cluster mode only.

Use the **no** form of the command to delete an NSX controller connection profile. All active connections are closed, and all tunnels related to this NSX controller are deleted.

By default, a connection profile is inactive. To activate a profile, run the **activate** command in NSX controller configuration mode.

Examples

To create an NSX controller profile named profile1:

```
switch# configure
switch(config)# nsx-controller profile1
```

nsx-controller name reconnect

Reconnects the NSX controller.

Syntax

nsx-controller name *name* **reconnect**

Parameters

name

Specifies the name for the NSX controller. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to reinitiate a connection to the specified NSX controller if the connection was broken. If the connection is already active, this command has no effect.

This command is available only for a switch that is in logical chassis cluster mode.

The specified NSX controller connection profile name must already exist.

Examples

To reconnect an NSX controller named nsx1:

```
sw0# nsx-controller name nsx1 reconnect
```

ntp authentication-key

Creates an authentication key to associate with the NTP server.

Syntax

ntp authentication-key *key-id* **md5** *md5-string* **encryption-level** *enc_value*

no ntp authentication-key *key-id*

Command Default

The default encryption-level is 7.

Parameters

key-id

Specifies an ID for an authentication key. The range is from 1 through 65535.

md5 *md5-string*

Specifies a string for the MD5 message-digest algorithm. The string can be a maximum of 15 alphanumeric characters.

encryption-level *enc_value*

Defines the level of encryption for the NTP authentication key. The valid values are 0 and 7. The value 0 is clear text format and the value 7 is fully encrypted format.

Modes

Global configuration mode

Usage Guidelines

This command adds an NTP authentication key (made up of a ID and an MD5 string) to a list of authentication keys in the database.

The maximum number of configurable NTP authentication keys is five. You cannot configure a duplicate key ID with a different key string. Use the **no ntp authentication-key** *key-id* command to remove the specified authentication key.

Before downgrading the firmware to a version that does not support the encryption-level option, the encryption-level should be set to 0.

Examples

To create an authentication key with an ID of 33 and an MD5 string called check:

```
switch# configure
switch(config)# ntp authentication-key 33 md5 check encryption-level 0
```

Related Commands

ntp server

ntp server

Specifies or adds an NTP server IP address and associates an authentication key to the server.

Syntax

ntp server *ip-address* [**key** *key-id*]

no ntp server *ip-address* [**key** *key-id*]

Command Default

The NTP server list is LOCL (no NTP server configured).

Parameters

ip-address
Specifies the NTP server IPv4 IP address (dot-decimal notation) or the IPv6 IP address (hexadecimal colon-separated notation).

key *key-id*
Associates a key from the key list to the specified server. The range for a key ID is from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Use this command to add an NTP server IPv4 or IPv6 address to a list of server IP addresses, or to associate an existing authentication key with an NTP server IP address.

The maximum number of NTP servers allowed is five.

Network Time Protocol (NTP) commands must be configured on each individual switch.

Use the **no ntp server** *ip-address* command to remove the specified NTP server IP address. Removing the current active NTP server resets the NTPstatus to "LOCL" until a new, active server is selected.

Use the **no ntp server** *ip-address* **key** *key-id* command to remove the key from the specified NTP IP address.

Examples

To associate a configured key ID of 15 to an NTP server:

```
switch(config)# ntp server 192.168.10.1 key 15
```

To remove an NTP server from the current list of NTP servers:

```
switch(config)# no ntp server 192.168.10.1
```

Related Commands

ntp authentication-key, show clock, show ntp status

ntp source-ip

Configures the source IP address to be used to access the NTP server.

Syntax

ntp source-ip [**chassis-ip** *ip_address* | **mm-ip** *ip_address*]

no ntp source-ip

Command Default

The NTP source IP is not configured.

Parameters

chassis-ip *ip_address*
Uses the IP address of the chassis for the NTP server.

mm-ip *ip_address*
Uses the management module (MM) IP address for the NTP server.

Modes

Global configuration mode

Usage Guidelines

Use the **no ntp source-ip** command to remove the configuration.

Examples

Typical command example:

```
switch# configure terminal
switch(config)# ntp source-ip chassis-ip 10.28.52.26
```

Typical command example:

```
switch# configure terminal
switch(config)# ntp source-ip mm-ip 10.28.52.27
```

History

Release version	Command history
5.0.2	This command was introduced.

oscmd

Provides a command shell for selected Linux commands.

Syntax

oscmd *Linuxcommand*

Parameters

Linuxcommand

The following Linux commands are supported with **oscmd** *:*

arp [**-a**]
Displays the Address Resolution Protocol (ARP) tables.

cat
Concatenates files and displays to standard output.

cp
Copies files and directories in a file system.

ftp
Transfers files to and from a remote server.

ifconfig [*netmask*] [**up**]
Configures the active network interface.

ls [**-al**] [*path*]
Lists files and directories on the switch.

mkdir *dir*
Creates a directory.

mv [**i**] *file1 file2*
Renames a file or directory.

rm [**-rf**] *file*
Removes a file or directory.

rmdir
Removes a directory.

tcpdump
Analyzes network traffic. The following parameters are supported with the Network OS implementation. Refer to the Linux documentation for more information on how to use this command. **-AbdDefIKlLnNOpqRStuUvxX**

- **-B** *buffer_size*
- **-c** *count*
- **-C** *file_size*
- **-G** *rotate_seconds*
- **-F** *file*
- **-i** *interface*

- **-m** *module*
- **-M** *secret*
- **-r** *file*
- **-s** *snaplen*
- **-T** *type*
- **-w** *file*
- **-W** *filecount*
- **-E** *spi@ipaddr*
- **-y** *datalinktype*
- **-z** *postrotate-command*
- **-Z** *user* [**expression**]

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to execute selected Linux commands on the switch. Refer to the Linux man pages for more information on the supported commands.

The **oscmd** command is disabled under FIPS mode.

Examples

To display the ARP table:

```
switch# oscmd arp -a

? (127.2.1.9) at ac:de:48:02:09:07 [ether] on eth2
? (127.2.1.7) at ac:de:48:02:07:07 [ether] on eth2
? (10.17.16.3) at 00:1b:ed:0b:90:00 [ether] on eth0
? (10.17.16.1) at 02:e0:52:5a:36:5c [ether] on eth0
? (10.17.19.14) at 00:14:22:20:5c:3c [ether] on eth0
? (127.2.2.9) at ac:de:48:02:09:08 [ether] on eth2
```

To copy a file to a remote server:

```
switch# oscmd rcp file root@127.2.1.8:

switch#
switch:FID128:root# telnet 127.2.1.8

Trying 127.2.1.8...
Connected to 127.2.1.8.
Escape character is '^]'.
Linux 2.6.34.6 (sw0) (0)
sw0 login: root

Password:
sw0:L2/0: >ls

.profile  .rhosts  file
```

To copy a file using secure copy:

```
switch# oscmd scp file file1 hegdes@10.31.2.27:

hegdes@10.31.2.27's password:  file
100%    0     0.0KB/s   00:00 file1
100%    0     0.0KB/s   00:00
```

overlay-gateway

Creates a VXLAN overlay gateway instance and enables VXLAN overlay gateway configuration mode.

Syntax

overlay-gateway *name*

no overlay-gateway *name*

Command Default

The default VXLAN overlay gateway setting for **type** is **nsx**.

Parameters

name

Specifies a name for the VXLAN overlay gateway. Only one gateway instance can be configured. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a VXLAN overlay gateway instance with the given name. An overlay network is a virtual network that is built on top of existing network Layer 2 and Layer 3 technologies. The objectives of setting up a gateway are:

- Configuring the source IP address
- Configuring the VLAN or VLANs
- Configuring MAC addresses to export to the VXLAN domain
- Enabling statistics collection for VLAN domains
- Enabling SPAN.

One you create the gateway instance, you enter VXLAN overlay gateway configuration mode, where you can configure other properties for this gateway. The key commands available in this mode are summarized below:

TABLE 9 Key commands available in VXLAN overlay gateway configuration mode

Command	Description
activate	Activates a VXLAN overlay gateway instance.
attach rbridge-id	Assigns a range of RBridge IDs to a VXLAN overlay gateway instance.
attach vlan	Specifies exported VLANs or MAC addresses in VXLAN overlay gateway configurations
enable statistics direction	Enables per-VLAN statistics collection for a VXLAN overlay gateway instance.
ip access-group	Sets an IPv4 ACL for the gateway.

TABLE 9 Key commands available in VXLAN overlay gateway configuration mode (continued)

Command	Description
ip interface loopback	Sets the loopback port number for the overlay gateway instance.
ip interface Ve	Sets the IP address of a VXLAN overlay gateway instance.
ipv6 access-group	Sets an IPv6 ACL for the gateway.
mac access-group	Sets a MAC ACL for the gateway.
map vlan vni	In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).
monitor session	Enables switched port analyzer (SPAN) on one or all tunnels of a VXLAN gateway.
sflow	Enables sFlow monitoring of the tunnel endpoints for a VXLAN overlay gateway.
site	Configures a remote Layer 2 extension site in a VXLAN overlay gateway context.
type	Specifies whether a VXLAN overlay gateway uses NSX Controller integration or Layer 2 extension.

This command is allowed for a switch that is in logical chassis cluster mode only.

Only one VXLAN overlay gateway instance can be configured.

Use the **no overlay-gateway** command to delete the VXLAN overlay gateway instance from the cluster. All tunnels for the gateway are also deleted. There are no other **no** forms of this command.

By default, a VXLAN overlay gateway instance is inactive. To activate an instance, first configure its other properties (such as which RBridges it attaches to), and then enter the **activate** command.

Note the following conditions related to changing the VXLAN gateway type:

- Before changing **type**, ensure that no RBridge is attached to the gateway.
- If changing **type** from **nsx** to **layer2-extension**, ensure that there are no "attach vlan" configurations.
- If changing **type** from **layer2-extension** to **nsx**, ensure that no "map vlan" configurations are present.

  NOTE
  The running configuration always shows the setting for **type**, even the default value (**nsx**). This means that when an overlay gateway is created, "type nsx" automatically appears in the running configuration.

Note the following conditions for related commands:

- The **attach vlan** command is valid only when **type** is **nsx**.
- The **map vlan vni** command is valid only when **type** is **layer2-extension**.

Examples

To create a VXLAN overlay gateway instance named "gateway1" and enter VXLAN overlay gateway configuration mode:

```
switch# config
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)#
```

Commands P through short-path-forwarding

password-attributes

Configures global password attributes.

Syntax

password-attributes [**min-length** *minlen*] [**max-retry** *maxretry*] [**character-restriction** [**upper** *numupper*] [**lower** *numlower*]] [**numeric** *numdigits*] [**special-char** *numsplchars*]]

no password-attributes [**min-length** *minlen*] [**max-retry** *maxretry*] [**character-restriction**]

Command Default

The default for *minlen* is 8. All other defaults are 0.

Parameters

min-length *minlen*

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

max-retry *maxretry*

Specifies the number of failed password logins permitted before a user is locked out. The lockout threshold range is 0 through 16. The default value is 0.

character-restriction

Configures the restriction on various types of characters.

upper *numupper*

Specifies the minimum number of uppercase alphabetic characters that must occur in the password. The default is 0, which means there is no restriction of uppercase characters.

lower *numlower*

Specifies the minimum number of lowercase alphabetic characters that must occur in the password. The default is 0, which means there is no restriction of lowercase characters.

numeric *numdigits*

Specifies the minimum number of numeric characters that must occur in the password. The number of numeric characters range is 0 through 32 characters. The default is 0.

special-char *numsplchars*

Specifies the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. The default value is 0.

Modes

Global configuration mode

Usage Guidelines

Enter **no password-attributes** *parameters* to set the specified password attributes to their default values.

Examples

To configure global password attributes and to verify the configuration:

```
switch(config)# password-attributes max-retry 4
switch(config)# password-attributes character-restriction lower 2
switch(config)# password-attributes character-restriction upper 1 numeric 1 special-char 1
switch(config)# exit
switch# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

To reset the character restriction attributes and to verify the configuration:

```
switch(config)# no password-attributes character-restriction lower
switch(config)# no password-attributes character-restriction upper
switch(config)# exit
switch# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction numeric 0
password-attributes character-restriction special-char 0
```

To clear the global password attributes:

```
switch(config)# no password-attributes
switch(config)# exit
switch# show running-config password-attributes

% No entries found.
```

Related Commands

rule, service password-encryption, show running-config password-attributes

password-attributes admin-lockout enable

Enables the lockout policy for admin role accounts.

Syntax

password-attributes admin-lockout enable

no password-attributes admin-lockout enable

Modes

Global configuration mode

Usage Guidelines

Lockout policy locks admin role accounts when the user exceeds the configured number of maximum failed login attempts.

In fabric cluster mode, when the **password-attributes admin-lockout enable** command is run on one switch of the cluster, it results in the configuration being applied to all switches of the cluster.

The **no password-attributes admin-lockout enable** command disables lockout policy for admin role accounts.

pdu-rx-limit

Sets the number of PDU packets received on an ELD-enabled port before detecting and breaking a loop.

Syntax

pdu-rx-limit *limit*

no pdu-rx-limit *limit*

Command Default

The default is 1.

Parameters

limit

The number of PDU packets. The valid range is 1 through 5.

Modes

ELD configuration mode

Usage Guidelines

This command sets the same value for every RBridge in the Brocade VCS Fabric cluster.

Use this command with the **hello-interval** command to determine the time taken to detect a loop. The time taken to detect a loop is the product of the pdu-rx-limit and the hello interval. The Brocade VCS Fabric cluster in the loop with the lowest pdu-rx-limit is the cluster where the loop gets broken, assuming that the hello limit is correctly set to the same value on all RBridges. This command applies only in Brocade VCS Fabric mode.

This functionality detects Layer 2 loops only.

Enter **no pdu-rx-limit** to reset the limit to its default value.

Examples

To set the limit on the number of PDU packets received to 4:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# pdu-rx-limit 4
```

Related Commands

edge-loop-detection vlan, edge-loop-detection port-priority, hello-interval, protocol edge-loop-detection, show edge-loop-detection globals

pg

Creates an N_Port group in Access Gateway mode.

Syntax

pg *pgid*

no pg *pgid*

Parameters

pgid

Port group identifier.

Modes

Access Gateway (AG) configuration mode

Usage Guidelines

You must be in Access Gateway (AG) mode to use this command.

This command configures a port group with a unique ID (pgid). The *pgid* cannot exceed 64 characters. Once configured, you can access the port group in Port Grouping configuration mode to perform configuration tasks, such as adding and removing N_Ports, enabling port group modes, and renaming the group.

Examples

The following command creates port group 1 and enables Port Grouping configuration mode for the port group.

```
sw0(config-rbridge-id-3-ag)# pg 1
sw0(config-rbridge-id-3-ag-pg-1)#
```

The following command removes port group 1.

```
sw0(config-rbridge-id-3-ag)# no pg 1
```

Related Commands

show ag pg

ping

Verifies network connectivity between a source and a destination on a TCP/IP network.

Syntax

ping *dest-IPv4_addr* [**ipv6** *dest-ipv6-addr*] [*host-name*] [**count** [*number*] [**interface** { *<N> gigabitethernet rbridge-id/slot/port*| **management** | **ve** *vlan_id* }]] [**timeout** *seconds*] [**datagram-size** *bytes*] [**quiet**] [**numeric**] [**vrf** *vrf-name*]

Command Default

The default for count is 5. The default for timeout is 1. The default for datagram-size is 56.

Parameters

dest-IPv4_addr
Specifies the IPv4 address of the destination device.

ipv6 *dest-ipv6-addr*
Specifies the IPv6 address of the destination device.

host-name
Destination host name. The default value is 1.

count *number*
Specifies the number of transmissions (pings). The range is from 1 through 7200.

interface*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port. The interface option is only available for the **ipv6 link-local address ping** command.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

interface management
Specifies the management interface.

interface Ve *vlan_id*
Specifies the interface is a virtual Ethernet, and specifies the VLAN ID of the interface.

timeout *seconds*
Specifies the time (in seconds) to wait for a response. The range is from 1 through 60. The default value is 1.

datagram-size *bytes*
Specifies the datagram size (also known as the maximum transmission unit, or MTU) in bytes. The range is from 36 through 9100. The default value is 56.

quiet
Prints only the first and last line of the command output.

numeric
Does not lookup hostnames.

vrf *vrf-name*
Pings the specified VRF instance. If no VRF is specified, the default-vrf is pinged. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

This command sends a specified number of pings with configured parameters to the specified destination device.

ATTENTION
Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management.

To ping management routes, use the **ping vrf** or **ping ipv6 vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually.

```
switch# ping vrf mgmt-vrf

switch# ping ipv6 vrf mgmt-vrf
```

Examples

To ping an IPv4 destination address:

```
switch# ping 172.16.4.80
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
64 bytes from 172.16.4.80: icmp_seq=0 ttl=120 time=101.466 ms
64 bytes from 172.16.4.80: icmp_seq=1 ttl=120 time=122.914 ms
64 bytes from 172.16.4.80: icmp_seq=2 ttl=120 time=145.637 ms
64 bytes from 172.16.4.80: icmp_seq=3 ttl=120 time=170.032 ms
64 bytes from 172.16.4.80: icmp_seq=4 ttl=120 time=103.036 ms
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 101.466/128.617/170.032/26.188 ms
```

To ping an IPv4 destination address in quiet mode:

```
switch# ping 172.16.4.80 quiet
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 100.605/146.372/192.552/32.505 ms
```

To ping an IPv6 destination address in numeric mode with a datagram size:

```
switch# ping ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 count 3 datagram-size 48
numeric timeout 3
Type Control-c to abort
PING fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470): 48
data bytes
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=0 ttl=64 time=6.356 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=1 ttl=64 time=0.170 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=2 ttl=64 time=0.171 ms
--- fec0:60:69bc:92:218:8bff:fe40:1470 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.170/2.232/6.356/2.916 ms
```

ATTENTION

Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management. This feature is allowed only on management VRF ports.

To ping management routes, use the **ping vrf** or **ping ipv6 vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually.

```
switch# ping vrf mgmt-vrf

switch# ping ipv6 vrf mgmt-vrf
```

Related Commands

traceroute

police cir

Sets the committed information rate for a class-map.

Syntax

police cir *cir-rate*

no police cir

Parameters

cir-rate

Committed information rate. Valid values range from 40000 through 40000000000 bps in multiples of 40000.

Modes

Policy-map class configuration mode

Usage Guidelines

When you are in config-policymap-class mode launching the **police cir cir-rate** command places the system in config-policymap-class-police mode for the configured class-map. At this point, you can add or remove additional policing parameters for the class-map.

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)#
```

Related Commands

cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, police-priority-map, policy-map, qos cos, service-policy, set-priority

police-priority-map

Creates color-based priority CoS mapping. A police-priority-map remaps frame CoS values to conform or exceed color values when rates conform or exceed limits set in a classification map.

Syntax

police-priority-map *name*

no police-priority-map *name*

conform *CoSvalues*

exceed *CoSvalues*

Command Default

If you do not define priority mapping for a color (conform or exceed), the map defaults to priorities 0, 1, 2, 3, 4, 5, 6, and 7.

Parameters

name
: Name of police-priority-map

CoSvalues
: CoS priority values (0, 1, 2, 3, 4, 5, 6, 7)

Modes

Global configuration mode

Police-priority-map configuration mode

Usage Guidelines

This command creates a police-priority-map.

When you launch the **police-priority-map** command, the system is placed in config-policepmap mode for the configured map. At this point, you can remap CoS values to conform or exceed color values.

Enter **conform** *CoSvalues* or **exceed** *CoSvalues* while in config-policepmap mode to remap 802.1p CoS values that are conforming to CIR values set in the policy-map or exceeding CIR values, but conforming to EIR values set in the policy-map.

Enter **no police-priority-map** *name* while in global configuration mode to remove the police-priority-map.

Enter **no conform** command or the **exceed** *CoSvalues* while in config-policepmap mode to remove CoS remapping.

NOTE
This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a priority-map and place system into config-policepmap mode to configure conform and exceed color mapping:

```
switch(config)# police-priority-map pmap1
switch(config-policepmap)# conform 0 1 1 2 1 2 1 1
switch(config-policepmap)# exceed 3 3 3 3 4 5 6 7
```

To remove the conform class mapping while in config-policepmap mode:

```
switch(config-policepmap)# no conform
```

To remove the class-map while in global configuration mode:

```
switch(config)# no police-priority-map pmap1
```

Related Commands

show running-config police-priority-map

policy-map

Configures a policy-map containing a class-map so that you can apply Policer and QoS attributes to a particular interface.

Syntax

policy-map *policy-mapname*

no policy-map *policy-mapname*

Command Default

No policy-map is created.

Parameters

policy-mapname
Name of police policy-map

Modes

Global configuration mode

Usage Guidelines

When you launch the **policy-map** command, the system is placed in config-policymap mode for the configured map. At this point, you can add a class-map containing policing parameters to the policy-map. (Refer to the description of the **class** command.)

This command creates a Policer policy-map to apply Policer and QoS attributes to a particular interface. Each policy-map can contain up to 32 class-maps. The class-map can be associated with specific policing and QoS parameters.

Maximum number of policy-map creations are 128

Associate the policy-map to the interface for inbound or outbound direction with the **service-policy** command.

Enter **no policy-map** *policy-mapname* while in global configuration mode to remove the policy-map.

NOTE
This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a policy-map and place system into config-policymap mode so that you can add a class-map:

```
switch(config)# policy-map policymap1
switch(config-policymap)#
```

To remove the policy-map while in global configuration mode:

```
switch(config)# no policy-map policymap1
```

Related Commands

class, qos cos, show policymap, show running-config class-map, show running-config policy-map

port-channel

Adds the port-channel as a member of a port-channel redundancy group.

Syntax

port-channel *po-id* [**active**]

no port-channel *po-id*

Modes

Port-channel-redundancy-group configuration mode

Usage Guidelines

Port-channel redundancy groups must have two port-channels as members and these port-channels can be from the same or different RBridges of a cluster.

You can specify which port-channel become active port-channel when this group gets activated. This is optional, if user doesn't provided active member, system will automatically select port-channel which comes up first as active.

The **no port-channel** command deletes the designated group.

Examples

Typical command execution example:

```
switch(config-port-channel-redundancy-group-32)# port-channel 3 active
```

Related Commands

port-channel-redundancy-group

port-channel-redundancy-group

Enables the port-channel-redundancy-group configuration mode.

Syntax

port-channel-redundancy-group *group-id*

no port-channel-redundancy-group *group-id*

Modes

Global configuration mode

Usage Guidelines

In this configuration mode, the **port-channel** command can add port-channels as members to the port-channel redundancy-group, and specify which port-channel becomes the active port-channel when the group is activated .

A port-channel redundancy group must have two port-channels as members. These port-channels can be from the same or different RBridges in a cluster. In the case of FC mode, the group configuration needs to be performed on all RBridges where any one of the vLAG members is configured.

Also in this configuration mode, the **activate** command activates this group.

The **no port-channel-redundancy-group command** deletes the designated group.

Examples

Typical command execution example:

```
switch(config)#port-channel-redundancy-group 27
switch(config-port-channel-redundancy-group-27)#
```

Related Commands

port-channel

port-channel path-cost

Sets the path-cost behavior.

Syntax

port-channel path-cost [**custom** | **standard**]

Command Default

Path-cost is standard.

Parameters

custom

Specifies to use the custom behavior, which sets the path-cost changes according to the port-channel's bandwidth.

standard

Specifies to use the standard behavior, which sets that the path-cost does not change according to port-channel's bandwidth.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all RBridges.

Examples

To set the behavior for the path-cost to custom:

```
switch(conf-mstp)# port-channel path-cost custom
```

To set the behavior for the path-cost to standard:

```
switch(conf-mstp)# port-channel path-cost standard
```

port-group

Enables port-group configuration mode for VDX 8770 Switch 27x40 GbE line cards. The mode is a prerequisite reserved for configuring Performance and Density operating modes on these line cards.

Syntax

port-group *rbridge-id/slot/port-group-id*

Parameters

rbridge-id

A unique identifier for the switch. Values are from 1 through 239.

slot

Specifies a valid slot number.

port-group-id

A port group number (1-9) specific to the Brocade VDX 8770 switch 27x40 GbE line card.

Modes

Hardware configuration mode

Usage Guidelines

When you launch the **port-group** command, the system is placed in configuration mode for the port group. At this point, you can configure Performance or Density operating modes for the port group.

Port groups on the 27x40 GbE line card are sequentially numbered starting with 1 for ports 1-3 and ending with 9 for ports 25-27. Refer to the *Brocade 8770-4 Hardware Reference Manual* or **8770-8 Hardware Reference Manual** "Overview" chapter for more information on these port groups and configuring operating modes for this line card.

NOTE

This command is only supported on 27x40 GbE line cards installed on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To enable port-group configuration mode for port group 9 on a line card located in slot 3 on a switch with RBridge ID 1:

```
switch(config-hardware)# port-group 1/3/9
switch(config-port-group-1/3/9)
```

Related Commands

hardware, port-group, mode (27x40 GbE line card)

port-profile (global configuration mode)

Creates a new Automatic Migration of Port Profiles (AMPP) port-profile in the fabric.

Syntax

port-profile *profile-name* [**activate** | **qos-profile** | **security-profile** | **vlan-profile** | **static** *mac-address*]

no port-profile *profile-name*

Parameters

profile-name
A fabric-wide unique name of a port-profile.

activate
Activates the specified profile

qos-profile
Enters directly into edit mode for the QoS sub-profile.

security-profile
Enters directly into edit mode for the security sub-profile.

vlan-profile
Enters directly into edit mode for the VLAN sub-profile.

static *mac-address*
Statically associates the profile VM MAC address.

Modes

Global configuration mode

Usage Guidelines

If the port-profile name already exists, the switch enters port-profile mode and edits the existing profile. A system-generated fabric-wide unique port-profile ID is assigned by default.

You can directly access the submodes for the profile, and assign the profile statically to a MAC address.

Security profiles are applied to the ACLs based on the profile or PolicyID. Therefore, multiple security profiles can be applied to the same profiled port.

Enter **no port-profile** *profile-name* to de-activate the port-profile.

port-profile (port-profile-domain configuration mode)

Adds an Automatic Migration of Port Profiles (AMPP) port-profile into a specific domain in a Virtual Fabrics context.

Syntax

port-profile *port-profile-name*

no port-profile *port-profile-name*

Parameters

port-profile-name

A fabric-wide unique name of a port-profile. Range is from 1 through 128 ASCII characters.

Modes

Port-profile-domain configuration mode

Usage Guidelines

You must first issue the **port-profile-domain** command to enter port-profile-domain configuration mode.

In a Virtual Fabrics context, use the **port-profile-port** command to associate a profiled port to a single port-profile or a port-profile domain.

Examples

Creating a port-profile in global configuration mode:

```
switch(config)# port-profile PP_Tenant_A
```

Creating a VLAN profile and enabling 802.1Q VLAN access on a trunk:

```
switch(config-port-profile-PP_Tenant_A)# vlan-profile
switch(config-vlan-profile)# switchport mode trunk allow vlan add 10
```

In a Virtual Fabrics context, creating extended VLAN profiles (VLAN IDs > 4095) to include service or transport VFs and C-TAGs.:

```
switch(config)# port-profile PP_Tenant_B
switch(config-vlan-profile)# switchport mode trunk allow vlan add 5000 ctag 20
switch(config-vlan-profile)# switchport mode trunk allow vlan add 6000 ctag 30
```

In a Virtual Fabrics context, adding port-profiles to a port-profile domain.

```
switch(config)# port-profile-domain vCenter1
switch(configport-profile-domain-vCenter1)# port-profile PP_Tenant_A
switch(configport-profile-domain-vCenter1)# port-profile PP_Tenant_B
```

Related Commands

port-profile-domain, vlan-profile (AMPP)

port-profile-domain

Creates an Automatic Migration of Port Profiles (AMPP) port-profile domain that contains all of the port-profiles that can be applied to a profiled port in a Virtual Fabrics context.

Syntax

port-profile-domain *port-profile-domain-name*

no port-profile-domain *port-profile-domain-name*

Parameters

port-profile-domain-name

A fabric-wide unique name of a port-profile domain. The range is from 1 through 128 ASCII characters.

Modes

Global configuration mode

Usage Guidelines

Within this domain, a service or transport VF (VLAN ID > 4095) must not have overlapping 802.1Q classification tags.

The **no** form of this command deletes a port-profile domain.

Use the **port-profile-port** command to associate a profiled port to a port-profile domain.

Examples

Creating a port-profile domain:

```
switch(config)# port-profile-domain my_PP_domain
```

Adding profiles to the above domain:

```
switch(config-port-profile-domain-my_PP_domain)# port-profile my_PP_domain_2
switch(config-port-profile-domain-my_PP_domain)# port-profile my_PP_domain_3
```

Related Commands

port-profile (global configuration mode), vlan-profile (AMPP)

port-profile-port

Activates the Automatic Migration of Port Profiles (AMPP) port-profile configuration mode on a port.

Syntax

port-profile-port [**domain** *port-profile-domain-name*]

no port-profile-port [**domain** *port-profile-domain-name*]

Command Default

When the **domain** keyword is not used, the port-profiles in the default profile domain are used.

Parameters

domain

Selects a port-profile domain.

port-profile-domain-name

Name of a port-profile domain.

Modes

Interface subtype configuration mode

Usage Guidelines

To apply multiple port-profiles to the interface, create and add the profiles to the default domain or to a user-created domain and apply it to the interface.

AMPP management allows you to associate AMPP port-profiles with VMware port groups, and provides a port-profile comparison tool to facilitate comparing port-profiles within or across fabrics for robust VM migration.

In a Virtual Fabrics context, use this command with the **domain** keyword to associate a profiled port to a port-profile domain. The result is that all service or transport VFs (VLAN ID > 4095) so specified are configured on the port.

- If multiple port-profiles are added to the default domain, use the **port-profile-port** command without the **domain** keyword.
- If multiple port-profiles are added to a user-created domain (for example, domain_d1), use the **domain** keyword as in the following example: **port-profile-port domain domain_d1**

When the **port-profile-port** command is issued without the **domain** keyword, the domain referred to is identified by "default." The default domain is automatically created by the system during a firmware upgrade from releases prior to Network OS release 4.1.0. When the upgrade is complete, this domain contains the set of port-profiles that were created before the upgrade.

Enter the **no port-profile-port** and **no shutdown** commands to remove the complete AMPP configuration from the selected port.

Enter **no port-profile-port domain** *port-profile-domain-name* to dissociate the profiled port from the port-profile domain.

NOTE
In VF-enabled mode only, the user can manage port-profiles in a default domain as in any other domain.

Examples

The following examples illustrate activating AMPP port-profile configuration mode on a specific 10-gigabit Ethernet interface port.

To associate the default port-profile domain to an interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# port-profile-port
```

To associate a profiled port with a user-specified port-profile domain:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# port-profile-port domain vDC1
```

Related Commands

interface, port-profile (global configuration mode), port-profile-domain, shutdown

power-off

Deactivates a line card or Switch Fabric Module (SFM).

Syntax

power-off { **linecard** | **sfm** } { *m4_value* | *m8_value* }

Parameters

linecard
Selects a line card to deactivate.

sfm
Selects an SFM to deactivate.

m4_value
The slot number. If you are using a Brocade VDX 8770-4 switch, the range of values is from 1 through 3.

m8_value
The slot number. If you are using a Brocade VDX 8770-8 switch, the range of values is from 1 through 6.

Modes

Global configuration mode

power-off linecard

Powers off a line card.

Syntax

power-off linecard *slot_number*

Parameters

slot_number

Specifies the slot number to be powered-off. Line card slots are 1 through 4 on a Brocade VDX 8770-4 and 1 through 8 on a Brocade VDX 8770-8.

Modes

Privileged EXEC mode

Usage Guidelines

A line card must be powered off before you can change the slot configuration.

Examples

To power off a line card in slot 4:

```
switch# power-off linecard 4
```

Related Commands

linecard, power-on linecard, show running-config rbridge-id linecard

power-on

Activates a line card or Switch Fabric Module (SFM).

Syntax

power-on { **linecard** | **sfm** } { *m4_value* | *m8_value* }

Parameters

linecard
Selects a line card to activate

sfm
Selects an SFM to activate.

m4_value
The slot number. If you are using a Brocade VDX 8770-4 switch, the range of values is from 1 through 3.

m8_value
The slot number. If you are using a Brocade VDX 8770-8 switch, the range of values is from 1 through 6.

Modes

Global configuration mode

power-on linecard

Powers on a line card.

Syntax

power-on linecard *slot_number*

Parameters

slot_number

Specifies the slot number to be powered-on. Line card slots are 1 through 4 on a Brocade VDX 8770-4 and 1 through 8 on a Brocade VDX 8770-8.

Modes

Privileged EXEC mode

Examples

To power on a line card in slot 4:

```
switch# power-on linecard 4
```

Related Commands

linecard, power-off linecard, show running-config rbridge-id linecard

precedence

Sets the precedence of the CEE map.

Syntax

precedence *value*

Command Default

The default is 1.

Parameters

value

The precedence value. Valid values range from 1 through 100.

Modes

CEE map configuration mode

Examples

To set the precedence to 1:

```
switch(config-cee-map-default)# precedence 1
```

preempt-mode

Enables or disables preempt mode for a VRRP router session.

Syntax

preempt-mode

no preempt-mode

Command Default

Enabled for VRRP; Disabled for VRRP-E.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command is for VRRP and VRRP-E.

For VRRP-E, the interface must be **ve**.

When set, the highest-priority backup router will always be the master if the owner is not available. If not set, a higher priority backup will not preempt a lower-priority master.

Enter **no preempt-mode** to turn off preempt mode.

Examples

To turn on preempt mode for a virtual-router-group-1 session:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# preempt-mode
```

Related Commands

vrrp-extended-group, vrrp-group

priority

Sets the priority of a physical router in a VRRP router group.

Syntax

priority *range*

Command Default

The default is 1.

Parameters

range

The priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers. Valid values range from 1 to 254.

Modes

Virtual-router-group configuration mode

Usage Guidelines

You can perform this command for VRRP or VRRP-E.

When set, the highest priority backup router will always be the master. (For VRRP, however, the owner is always the master if it is available.) If not set, a higher priority backup will not preempt a lower priority backup that is acting as master.

For an owner router in VRRP, the priority automatically becomes 255 if the virtual IP address of the virtual router and the real IP address of the owner are the same.

Examples

To set the priority to 110 for the VRRP virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# priority 110
```

To set the priority to 110 for the VRRP-E virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp-extended
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-group-extended 1
switch(config-vrrp-extended-group-1)# priority 110
```

Related Commands

vrrp-extended-group, vrrp-group

priority-group-table

Configures the bandwidth for each priority group.

Syntax

priority-group-table *pgid* [**weight** *weight*] [**pfc** { **on** | **off** }]

no priority-group-table *pgid*

Command Default

There is no default value for the weight. PFC is disabled.

Parameters

pgid

Specifies the priority group ID (PGID) assigned to a priority group. Valid values range from 15.0 through 15.7 for the eight reserved Strict Priority PGIDs.

weight *weight*

Maps a weight to a Deficit Weighted Round Robin (DWRR) scheduler queue. This parameter is only valid for the DWRR Priority Group. The sum of all DWRR Priority Group weight values must equal 100 percent. Valid values range from 1 through 100.

pfc

Enables the Priority-based Flow Control (PFC) for each priority that gets mapped to the priority group.

on

Enables PFC.

off

Disables PFC.

Modes

CEE map configuration mode

Usage Guidelines

Enter **priority-group-table** to configure the bandwidth for each priority group, to associate a weight to a DWRR scheduler queue, and to enable the PFC.

You can define up to eight additional DWRR Priority Groups with the PGID values in the range from 0 through 7. Strict Priority Groups take priority in order from the lowest PGID value to the highest PGID value; for example, a PGID of 15.0 is a higher priority than a PGID of 15.1 and a PGID of 15.1 is higher priority than a PGID of 15.2.

Enter **no priority-group-table** *pgid* to return the priority group to the default values. For the Strict Priority Group, the PGID is still valid, but the PFC is disabled. For the DWRR Priority Group, the PGID is no longer valid and is deleted; the PGID can only be deleted when it is not bound to any Priority-to-Priority Group Table entry. The following lists the bandwidth allocation to user priority groups.

TABLE 10 Bandwidth allocation to user priority groups

PGID	PG%	PFC	Description
0	50	Y	SAN
1	50	N	LAN

A PGID value of 15 is a special value, which allows you to configure priorities with no bandwidth limit. The priority groups of 15.0 to 15.7 are predefined in the switch.

Examples

To define the CEE map and configure the bandwidth with the priority group, use the values in Table 10.

```
switch(config)# cee-map test
switch(conf-ceemap)# priority-group-table 0 weight 50 pfc on
switch(conf-ceemap)# priority-group-table 1 weight 50
```

Related Commands

cee-map (FCoE), show qos maps, show running-config cee-map

priority-tag

Toggles the priority-tagging support on a specific interface.

Syntax

priority-tag

no priority-tag

Command Default

The priority-tag is disabled for all supported interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is the only method for toggling priority-tagging.

Enter **no priority-tag** to disable priority-tagging support.

Examples

To enable priority-tagging support on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# priority-tag
```

Related Commands

interface, cee-map (FCoE)

private-vlan

Configures a VLAN as a private VLAN (PVLAN).

Syntax

private-vlan [**isolated** | **community** | **primary**]

no private-vlan [**isolated** | **community** | **primary**]

Parameters

isolated
The PVLAN is configured as an Isolated VLAN.

community
The PVLAN is configured as a Community VLAN.

primary
The PVLAN is configured as a Primary VLAN.

Modes

Interface subtype configuration mode

Related Commands

private-vlan association

private-vlan association

Associates a secondary VLAN to a primary VLAN.

Syntax

private-vlan association [**add** *vlan_id* | **remove** *vlan_id*]

no private-vlan association [**add** *vlan_id* | **remove** *vlan_id*]

Parameters

add *vlan_id*
: Adds the association.

remove *vlan_id*
: Removes the association.

Modes

Interface subtype configuration mode

Related Commands

private-vlan

profile

Creates an LLDP profile.

Syntax

profile *name*

no profile *name*

Parameters

name

Assigns a name to the profile. The name must be between 1 and 63 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile. Up to 64 profiles can be created.

Enter **no profile** *name* to remove the named profile.

Examples

To create a profile named test:

```
switch(conf-lldp)# profile test
```

To delete a profile named test:

```
switch(conf-lldp)# no profile test
```

Related Commands

lldp profile

prom-access disable

Disables access to the Boot PROM for FIPS compliance.

Syntax

prom-access disable

Command Default

The Boot PROM is accessible.

Modes

Privileged EXEC mode

Usage Guidelines

In non-FIPS compliant mode, you can access the Boot PROM by holding down the ESC key during the 4-second period when the switch is booting up. In FIPS compliant state, PROM access is disabled to prevent users from net-installing firmware.

Under normal operating conditions, this command is hidden to prevent accidental use. Enter **unhide fips** with the password "fibranne" to make the command available.

ATTENTION
Use this command only when preparing a switch for FIPS compliance.

CAUTION
Once Boot PROM access is disabled, you cannot re-enable it.

Examples

To disable access to the Boot PROM:

```
switch# unhide fips

Password: *****

switch# prom-access disable

You are disabling PROM access. Do you want to continue? [yes/no] (no): yes

switch# PROM access Disabled
```

Related Commands

cipherset, fips selftests, fips zeroize, show prom-access, unhide fips

protect-mode enable

Enables protect mode.

Syntax

protect-mode enable

no protect-mode enable

Modes

Privileged EXEC mode

Usage Guidelines

In the Blade Center Chassis environment, the Advanced Management Module (AMM) controls the operation of the switch by configuring and initializing it. Protect mode of operation is a special mode which needs to be supported by both the switch and the AMM. Protect mode results in the AMM ceding control to the switch. The AMM loses its ability to perform some or all of the operations on the AMM. Once the AMM cedes control to the switch, the control can be given back to the AMM only by disabling protect mode on the switch.

Once the switch enters protect mode, AMM's requests to perform any operations are ignored until the Network Administrator permits them. This behavior is preserved through power cycles, even after it is inserted into a different bay or chassis.

Enter **no protect-mode enable** to disable this command.

protocol edge-loop-detection

Sets the edge-loop detection (ELD) configuration mode.

Syntax

protocol edge-loop-detection

Command Default

ELD configuration mode is not set.

Modes

Global configuration mode

Usage Guidelines

This functionality detects Layer 2 loops only.

Examples

To enter the ELD configuration mode:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)#
```

Related Commands

hello-interval, pdu-rx-limit, shutdown-time

protocol lldp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

Syntax

protocol lldp

no protocol lldp

Command Default

The LLDP and DCBX protocols are enabled.

Modes

Global configuration mode

Usage Guidelines

Enter **no protocol lldp** to restore the default settings.

Examples

To reset all LLDP configurations:

```
switch(config)# no protocol lldp
```

protocol spanning-tree

Designates the context for spanning tree.

Syntax

protocol spanning-tree { **mstp** | **rstp** | **stp** | **pvst** | **rpvst** }

no protocol spanning-tree

Command Default

STP is not enabled. STP is not required in a loop-free topology.

Parameters

mstp
Specifies the Multiple Spanning Tree Protocol (MSTP).

rstp
Specifies the Rapid Spanning Tree (RSTP).

stp
Specifies the Spanning Tree Protocol (STP).

pvst
Specifies Per-VLAN Spanning Tree Protocol Plus (PVST+).

rpvst
Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

Modes

Global configuration mode

Usage Guidelines

Consider enabling STP to detect or avoid loops. You must turn off one form of STP before turning on another form.

Packet drops or packet flooding may occur if you do not enable xSTP on all devices connected on both sides of parallel links.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no protocol spanning-tree** to delete the context and all the configurations defined within the context or protocol for the interface.

Examples

To enable the Spanning Tree Protocol:

```
switch(config)# protocol spanning-tree stp
```

Related Commands

show spanning-tree

protocol udld

Enables and/or enters unidirectional link detection (UDLD) protocol configuration mode.

Syntax

protocol udld

no protocol udld

Command Default

This protocol is disabled by default.

Modes

Global configuration mode

Usage Guidelines

UDLD detects and blocks a physical link that becomes unidirectional. A unidirectional link can cause traffic in a network to loop endlessly. When the link becomes bidirectional again, UDLD unblocks the link.

This protocol applies only to physical ports. In addition to running this command, you must also enable each desired port for UDLD in interface subconfiguration mode.

Use the **no protocol udld** command to disable the UDLD protocol and revert all UDLD configuration to defaults.

Examples

To enable the unidirectional link detection (UDLD) protocol:

```
switch# configure
switch(config)# protocol udld
```

Related Commands

hello (UDLD), udld enable, shutdown (UDLD)

protocol vrrp

Globally enables VRRP (and VRRP-E on some platforms).

Syntax

protocol vrrp

no protocol vrrp

Command Default

Disabled

Modes

RBridge ID configuration mode

Usage Guidelines

Enables both the VRRP and VRRP-Extended protocols on the Brocade VDX switch.

The **no protocol vrrp** command globally disables only VRRP but not VRRP-E.

Examples

To enable VRRP and VRRP-E:

```
switch# configure
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
```

Related Commands

protocol vrrp-extended

protocol vrrp-extended

Globally enables VRRP-Extended.

Syntax

protocol vrrp-extended

no protocol vrrp-extended

Command Default

Disabled

Modes

RBridge ID configuration mode

Usage Guidelines

The **no protocol vrrp-extended** command globally disables VRRP-Extended.

Examples

To enable VRRP-Extended:

```
switch# configure
switch (config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp-extended
```

Related Commands

protocol vrrp

pwd

Displays the mode of the current working directory.

Syntax

pwd

Modes

Functions in all modes except privileged EXEC mode.

Examples

To view the current working directory:

```
switch2# pwd

---------^
syntax error: unknown argument.
switch# configure terminal

Entering configuration mode terminal
switch(config)# pwd

At top level
switch(config)#
```

qos

If there is bursty, lossy traffic for certain flows in the system, you can borrow the buffers from less bursty flows, in order to reduce the traffic loss. The **qos** command is used to configure the egress or ingress queue limit (depth), such as the maximum number of kilobytes of data that can be queued in the egress or ingress queue. This configuration is applied on individual RBridges.

Syntax

qos { **tx-queue** | **rcv-queue**} [**limit** *limitInKBytes*]

no qos

Command Default

The range of queue limit values is from 128 KB through 8 MB. While any value within this range is valid, recommended values are 128, 256, 512, 1024, and 2048.

The default ingress queue limit is 285 kilobytes.

The default egress queue limit is 512 kilobytes.

Parameters

tx-queue
Designates the egress queue.

rcv-queue
Designates the ingress queue.

limit *limitInKBytes*
Configures the limit of the queue in kilobytes.

Modes

RBridge ID configuration mode

Usage Guidelines

The **no qos** command removes both queue limits and the default queue limits are restored.

This command only functions on the Brocade VDX 6740 and the Brocade VDX 6740-T

Examples

This example defines the egress queue to 512 kilobytes.

```
(config-rbridge-id-154)# qos tx-queue limit 512
```

History

Release version	Command history
5.0.0	This command was introduced.

qos cos

Specifies the interface Class of Service (CoS) value.

Syntax

qos cos *value*

no qos cos

Command Default

The default is 0.

Parameters

value

Specifies the CoS value. Valid values range from 0 through 7.

Modes

Interface subtype configuration mode

Usage Guidelines

When Interface ingress QoS Trust is in the un-trusted mode, then the Interface Default CoS value is applied to all ingress traffic for user priority mapping. When the interface ingress QoS Trust is in the CoS mode, then the Interface Default CoS value is applied to all nonpriority tagged ingress traffic for user priority mapping.

If the interface is QoS trusted, the CoS value of the interface is used to assign a CoS value to all untagged packets entering the interface.

QoS Trust is implicitly turned on when the QoS CoS-Mutation map is applied to interfaces, and is implicitly turned off when the QoS CoS-Mutation map is removed.

Enter **no qos cos** to return the CoS value to the default.

Examples

To set the CoS value to 2 on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# qos cos 2
```

To return the CoS value to the default on a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-port-channel-22)# no qos cos
```

Related Commands

interface, qos map cos-traffic-class, qos trust cos, show qos interface

qos cos-mutation

Applies a CoS-to-CoS mutation quality of Service (QoS) map on an interface.

Syntax

qos cos-mutation *name*

no qos cos-mutation

Command Default

No explicit CoS-to-CoS mutation QoS map is applied; the inbound CoS equals the outbound CoS.

Parameters

name

Specifies the name of the CoS mutation map.

Modes

Interface subtype configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

The **qos cos-mutation** command is not available if the interface is in CEE Provisioning mode.

Enter **no qos cos-mutation** to remove the CoS-to-CoS mutation map.

Examples

To activate a CoS-to-CoS mutation QoS map named *test* on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# qos cos-mutation test
```

To remove a CoS-to-CoS mutation QoS map from a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-port-channel-22)# no qos cos-mutation
```

Related Commands

interface, qos map cos-mutation, show qos maps

qos cos-traffic-class

Applies a CoS-to-Traffic Class QoS map on an interface.

Syntax

qos cos-traffic-class *name*

no qos cos-traffic-class

Command Default

No explicit CoS-to-Traffic Class QoS map is applied; the implicit behavior is to match the IEEE 802.1Q recommendations for systems supporting 8 Traffic Classes.

Parameters

name

Specifies the name of a previously created CoS-to-Traffic Class QoS map. Only one CoS-to-Traffic Class QoS map can exist at a time. An existing CoS-to-Traffic Class QoS map must be removed before a new one can be applied.

Modes

Interface subconfiguration mode (fo, gi, port-channel, te)

Usage Guidelines

This command is not available when the interface is in the CEE provisioning mode.

Enter **no qos cos-traffic-class** to remove the CoS-to-Traffic Class mapping.

Examples

To apply a CoS-to-Traffic Class QoS map named 'test'to a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos cos-traffic-class test
```

To remove CoS-to-Traffic Class QoS mapping from a specific port-channel interface:

```
switch(config)# interface port-channel 22
switch(config-port-channel-22)# no qos cos-traffic-class
```

Related Commands

interface, qos cos-mutation, qos map cos-traffic-class, qos trust cos, show qos maps

qos dscp-cos

Applies a defined DSCP-CoS map to an interface.

Syntax

qos dscp-cos *name*

no qos dscp-cos

Command Default

DSCP-to-CoS mutation is not enabled on interface.

Parameters

name

Name of DSCP-to-COS mutation map

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no qos dscp-cos** while in the interface mode to remove the DSCP-CoS map from the interface.

Examples

To apply a configured QoS dscp-mutation map named 'test' to a specific interface, enter the **qos dscp-cos** *name* command while in the interface subconfiguration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-cos test
```

To remove a configured QoS dscp-mutation map named 'test' from a specific interface, enter the **no qos dscp-cos** command while in the interface subconfiguration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-cos
```

Related Commands

interface, qos dscp-mutation, qos map dscp-cos, qos dscp-cos, show qos maps dscp-cos

qos dscp-mutation

Applies a defined DSCP mutation map to an interface.

Syntax

qos dscp-mutation *name*

no qos dscp-mutation

Command Default

DSCP mutation map is not enabled on interface.

Parameters

name

Name of DSCP mutation map

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no qos dscp-mutation** while in the interface mode to remove the DSCP mutation map from the interface.

Examples

To apply a configured QoS dscp-mutation map named 'test' to a specific interface, enter the **qos dscp-mutation** *name* command while in the interface mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-mutation test
```

To remove a configured QoS dscp-mutation map named 'test' from a specific interface, enter the **no qos dscp-mutation** *name* command while in the interface mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-mutation
```

Related Commands

interface, qos map dscp-mutation, show qos maps dscp-mutation

qos dscp-traffic-class

Applies a defined DSCP-to-Traffic-Class map to an interface.

Syntax

qos dscp-traffic-class *name*

no qos dscp-traffic-class

Command Default

DSCP-to-Traffic-Class map is not enabled on the interface.

Parameters

name

Name of DSCP-to-Traffic-Class map

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no qos dscp-traffic-class** while in the interface mode to remove the DSCP-to-Traffic-Class map from the interface.

Examples

To apply a configured DSCP-Traffic-Class map named 'test' to a specific interface, enter **qos dscp-traffic-class** *name* while in the interface configuration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# qos dscp-traffic-class test
```

To remove a configured DSCP-Traffic-Class map named 'test' from a specific interface, enter **no qos dscp-traffic-class** while in the interface configuration mode:

```
switch(config)# interface tengigabitethernet 16/2/2
switch(conf-if-te-16/2/2)# no qos dscp-traffic-class
```

Related Commands

interface, qos map dscp-traffic-class, show qos maps dscp-traffic-class

qos flowcontrol

Activates and configures QoS flow control.

Syntax

qos flowcontrol tx [**on** | **off**] **rx** [**on** | **off**]

no qos flowcontrol

Parameters

tx [**on** | **off**]

Activates or deactivates the transmission portion of flow control.

rx [**on** | **off**]

Activates or deactivates the receiving portion of flow control.

Modes

Interface subtype configuration mode

Usage Guidelines

When a 1-Gbps local port is already online, and the **qos flowcontrol** command is issued, the pause settings take effect immediately on that local port. However, when the link is toggled, pause is renegotiated. The local port will advertise the most recent **qos flowcontrol** settings. After auto completes, the local port pause settings may change, depending on the outcome of the pause negotiation, per 802.3 Clause 28B, as shown below.

TABLE 11 Pause negotiation results

Advertised LOCAL cfg	Advertised REMOTE cfg	Negotiated result
Rx=off Tx=on	Rx=on Tx=on	asymmetrical: LOCAL Tx=on --> pause --> REMOTE Rx=on
Rx=on Tx=on	Rx=off Tx=on	asymmetrical: LOCAL Rx=on <-- pause <-- REMOTE Tx=on
Rx=on Tx=n/a	Rx=on Tx=n/a	symmetrical : LOCAL Tx/Rx=on <-- pause --> REMOTE Tx/Rx=on
Rx=n/a Tx=n/a	Rx=off Tx=off	disable pause both sides

Enter **no qos flowcontrol** to deactivate flow control on a specific interface.

Examples

To activate both the transmitting and receiving portions of flow control on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-fo-1/3/1)# qos flowcontrol tx on rx on
```

To deactivate flow control on a specific port-channel interface:

```
switch(config)# interface port-channel 33
switch(config-port-channel-33)# no qos flowcontrol
```

Related Commands

interface

qos flowcontrol pfc

Activates and configures flow control for a Class of Service (CoS).

Syntax

qos flowcontrol pfc *cos_value* **tx** [**on** | **off**] **rx** [**on** | **off**]

no qos flowcontrol pfc *cos_value*

Parameters

cos_value
The CoS value.

tx [**on** | **off**]
Activates or deactivates the transmission portion of flow control.

rx [**on** | **off**]
Activates the receiving portion of flow control.

Modes

Interface subtype configuration mode

Usage Guidelines

In Brocade VCS Fabric mode, this command:

- Only takes effect on the interface. In order to have PFC functionality through the Brocade VCS Fabric cluster, use the CEE map configuration.
- Only affects per-interface pause behavior. To use flow control in Brocade VCS Fabric mode, use the CEE map configuration.

Enter **no qos flowcontrol pfc** *cos_value* to deactivate CoS flow control on a specific interface.

Examples

To activate both the transmitting and receiving portions of a Class of Service (with a value of 7 in this example) flow control on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-fo-1/3/1)# qos flowcontrol pfc 7 tx on rx on
```

To deactivate both the transmitting and receiving portions of a Class of Service (with a value of 4 in this example) flow control on a specific port-channel interface:

```
switch(config)# interface port-channel 33
switch(config-port-channel-33)# no flowcontrol pfc 4
```

Related Commands

interface

qos map cos-mutation

Creates a QoS map for performing CoS-to-CoS mutation.

Syntax

qos map cos-mutation *name cos0 cos1 cos2 cos3 cos4 cos5 cos6cos7*

no qos map cos-mutation *name*

Command Default

No CoS-to-CoS mutation QoS maps are defined.

Parameters

name

Specifies a unique name across all CoS-to-CoS mutation QoS maps defined within the system. If the named CoS-to-CoS mutation QoS map does not exist, then it is created. If the named CoS-to-CoS mutation QoS map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the QoS map.

cos0

Sets the outbound CoS value for all packets with inbound CoS 0.

cos1

Sets the outbound CoS value for all packets with inbound CoS 1.

cos2

Sets the outbound CoS value for all packets with inbound CoS 2

cos3

Sets the outbound CoS value for all packets with inbound CoS 3.

cos4

Sets the outbound CoS value for all packets with inbound CoS 4.

cos5

Sets the outbound CoS value for all packets with inbound CoS 5.

cos6

Sets the outbound CoS value for all packets with inbound CoS 6.

cos7

Sets the outbound CoS value for all packets with inbound CoS 7.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-CoS mutation takes an inbound CoS value and maps it to an outbound CoS value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied. The outbound CoS value is used in selecting Traffic Class and egress packet marking.

Enter **no qos map cos-mutation** *name* command to delete the named CoS-to-CoS mutation QoS map. A QoS map can only be deleted if it is not bound to any interface.

Examples

To create a CoS-to-CoS mutation QoS map to swap CoS 4 and CoS 5 and apply it on an interface, for example having inbound CoS 4 mapped to outbound CoS 5 and inbound CoS 5 mapped to outbound CoS 4; but all other CoS values go through unchanged:

```
switch(config)# qos map cos-mutation test 0 1 2 3 5 4 6 7
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# qos cos-mutation test
```

To delete a CoS-to-CoS mutation QoS map:

```
switch(config)# no qos map cos-mutation test
```

Related Commands

qos cos-mutation, show qos maps

qos map cos-traffic-class

Creates a QoS map for performing CoS-to-Traffic Class mapping.

Syntax

qos map cos-traffic-class *name tc0 tc1 tc2 tc3 tc4 tc5 tc6tc7*

no qos map cos-traffic-class

Command Default

No CoS-to-Traffic Class QoS maps are defined.

Parameters

name

Specifies the CoS-to-Traffic Class QoS map name. If the named CoS-to-Traffic Class QoS map does not exist, then it is created. If the named CoS-to-Traffic Class QoS map already exists, then it is updated and new mappings are automatically propagated to all interfaces bound to the QoS map.

tc0

Sets the Traffic Class value for all packets with outbound CoS 0.

tc1

Sets the Traffic Class value for all packets with outbound CoS 1.

tc2

Sets the Traffic Class value for all packets with outbound CoS 2.

tc3

Sets the Traffic Class value for all packets with outbound CoS 3.

tc4

Sets the Traffic Class value for all packets with outbound CoS 4.

tc5

Sets the Traffic Class value for all packets with outbound CoS 5.

tc6

Sets the Traffic Class value for all packets with outbound CoS 6.

tc7

Sets the Traffic Class value for all packets with outbound CoS 7.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-Traffic Class QoS map takes an outbound CoS value and maps it to a Traffic Class. The outbound CoS value is used as the packet user priority after applying the configured interface QoS trust, interface default CoS, and CoS-to-CoS mutation policies. Traffic Class is a reference to a scheduler queue and packet servicing policy.

Enter **no qos map cos-traffic-class** *name* to delete the CoS-to-Traffic Class QoS map specified by *name*. The CoS-to-Traffic Class QoS map can only be deleted when it is not bound to any interface. All other CoS values go through unchanged. This mapping matches the default behavior recommended in IEEE 802.1Q for systems supporting 8 Traffic Classes.

Examples

To create a CoS-to-Traffic Class QoS map to map CoS 0 to Traffic Class 1 and CoS 1 to Traffic Class 0:

```
switch(config)# qos map cos-traffic-class test 1 0 2 3 4 5 6 7
```

To delete a CoS-to-Traffic Class QoS map:

```
switch(config)# no qos map cos-traffic-class test
```

Related Commands

qos map cos-mutation, qos trust cos

qos map dscp-cos

Creates a QoS map for performing DSCP-to-CoS mapping. This configures a DSCP-to-CoS map on the ingress interface.

Syntax

qos map dscp-cos *name*

no qos map dscp-cos *name*

mark *ingress dscp values* **to** *egress cos value*

Command Default

DSCP-to-CoS mutation is not enabled.

Parameters

name
Name of dscp-cos map

ingress dscp values
Range of input DSCP values

egress dscp values
Output CoS value

Modes

dscp-cos mode for the QoS map

Global configuration mode

Usage Guidelines

This command remaps the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

When you enter **qos map dscp-cos**, the system is placed in dscp-cos mode for the configured map. At this point, you can map ingress DSCP values to egress CoS values using the **mark** command.

Enter **qos dscp-cos** *name* while in configuration mode for a specific interface to apply the DSCP-CoS map to that interface.

Enter **no qos dscp-cos** *name* while in the interface configuration mode to remove the map from the interface.

Enter **no map dscp-cos** *name* while in global configuration mode to remove the DSCP-CoS map.

Examples

To create a QoS DSCP-CoS map and place system into dscp-cos mode:

```
switch(config)# qos map dscp-cos test
switch(dscp-cos-test)#
```

To map an ingress DSCP value to egress CoS values while in dscp-cos mode:

```
switch(dscp-cos-test)# mark 1,3,5,7 to 3
```

To map multiple ingress DSCP values to egress CoS values while in dscp-cos mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
switch(dscp-mutation-test)# mark 11,13,15,17 to 5
switch(dscp-mutation-test)# mark 12,14,16,18 to 6
switch(dscp-mutation-test)# mark 2,4,6,8 to 7
```

To remove a QoS DSCP-CoS map while in global configuration mode:

```
switch(config)# no qos map dscp-cos test
```

Related Commands

qos map dscp-traffic-class, qos dscp-cos, show qos maps dscp-cos

qos map dscp-mutation

Creates a DSCP mutation by remapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

Syntax

qos map dscp-mutation *name*

no map qos dscp-mutation *name*

mark *ingress dscp values* **to** *egress dscp value*

Command Default

DSCP mutation is not enabled.

Parameters

name
Name of dscp-mutation map

ingress dscp values
Range of input DSCP values

egress dscp values
Output DSCP value

Modes

dscp-mutation mode for the dscp-mutation map

Global configuration mode

Usage Guidelines

Enter **qos dscp-mutation** *name* while in configuration mode for a specific interface to apply the dscp-mutation map to that interface. When you enter **qos map dscp-mutation**, the system is placed in dscp-mutation mode for the configured map. At this point, you can map ingress DSCP values to egress DSCP values using the **mark** command.

Enter **no qos dscp-mutation** *name* while in interface configuration mode to remove the map from that interface.

Enter **no map dscp-mutation** *name* while in global configuration mode to remove the dscp-mutation map.

NOTE
This command is only supported on VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a QoS DSCP-mutation map and place system into dscp-mutation mode:

```
switch(config)# qos map dscp-mutation test
switch(dscp-mutation-test)#
```

To map an ingress DSCP value to egress DSCP values while in dscp-mutation mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
```

To map multiple ingress DSCP values to egress DSCP values while in dscp-mutation mode:

```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
switch(dscp-mutation-test)# mark 11,13,15,17 to 19
switch(dscp-mutation-test)# mark 12,14,16,18 to 20
switch(dscp-mutation-test)# mark 2,4,6,8 to 10
```

To remove a QoS DSCP-mutation map while in global configuration mode:

```
switch(config)# no qos map dscp-mutation test
```

Related Commands

qos dscp-mutation, show qos maps dscp-mutation

qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-Traffic Class mapping. This creates a dscp-traffic-class map on the ingress interface. You can configure an interface with either a DSCP-to-Traffic-Class map or a CoS-to-Traffic-Class map.

Syntax

qos map dscp-traffic-class *name*

no qos map dscp-traffic-class *name*

mark *ingress dscp values* **to** *traffic class*

Command Default

DSCP-to-Traffic-Class mutation is not enabled.

Parameters

name
Name of QoS DSCP-to-Traffic Class map.

ingress dscp values
Range of input DSCP values

traffic class
Traffic Class (0-7)

Modes

dscp-traffic-class mode for the dscp-traffic-class map

Global configuration mode

Usage Guidelines

Enter **qos dscp-traffic-class** *name* while in configuration mode for a specific interface to apply the QoS DSCP-Traffic-Class map to that interface. When you enter **qos map dscp-traffic-class**, the system is placed in dscp-traffic-class mode for the configured map. At this point, you can map ingress DSCP values to traffic class values using the **mark** command.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

Enter **no map dscp-mutation** *name* to remove the map while in global configuration mode.

Examples

To create a QoS DSCP-Traffic-Class map and place system into dscp-traffic-class mode:

```
switch(config)# qos map dscp-traffic-class test
switch(dscp-traffic-class-test)#
```

To map ingress DSCP values to a traffic class while in dscp-traffic-class mode:

```
switch(dscp-traffic-class-test)# mark 1,3,5,7 to 3
```

To map multiple ingress DSCP values to traffic classes while in dscp-traffic-class mode:

```
switch(dscp-traffic-class-test)# mark 1,3,5,7 to 3
switch(dscp-traffic-class-test)# mark 11,13,15,17 to 5
switch(dscp-traffic-class-test)# mark 12,14,16,18 to 6
switch(dscp-traffic-class-test)# mark 2,4,6,8 to 7
```

To remove a QoS DSCP-Traffic-Class map while in global configuration mode:

```
switch(config)# no qos map dscp-traffic-class test
```

Related Commands

qos dscp-traffic-class, show qos maps dscp-traffic-class

qos queue multicast scheduler

Configures the multicast Traffic Class packet expansion scheduler policy. All multicast Traffic Class packet expansion queues are serviced Deficit Weighted Round Robin (DWRR).

Syntax

qos queue multicast scheduler dwrr *mTC0_WEIGHT mTC1_WEIGHT mTC2_WEIGHT mTC3_WEIGHT mTC4_WEIGHT mTC5_WEIGHT mTC6_WEIGHT mTC7_WEIGHT*

no qos queue multicast scheduler

Command Default

The default weight value is 25 percent bandwidth for each multicast Traffic Class.

Parameters

dwrr

Configures the DWRR multicast Traffic Class packet expansion policy.

mTC0_WEIGHT

Sets the DWRR weight for multicast Traffic Class 0 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC1_WEIGHT

Sets the DWRR weight for multicast Traffic Class 1 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC2_WEIGHT

Sets the DWRR weight for multicast Traffic Class 2 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC3_WEIGHT

Sets the DWRR weight for multicast Traffic Class 3 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC4_WEIGHT

Sets the DWRR weight for multicast Traffic Class 4 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC5_WEIGHT

Sets the DWRR weight for multicast Traffic Class 5 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC6_WEIGHT

Sets the DWRR weight for multicast Traffic Class 6 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

mTC7_WEIGHT

Sets the DWRR weight for multicast Traffic Class 7 packet expansion in units of bandwidth percentage. The sum of all weight values must equal 100 percent. Valid values range from 0 through 100.

Modes

Global configuration mode

Usage Guidelines

All multicast Traffic Class packet expansion queues are serviced Deficit Weighted Round Robin (DWRR). This multicast Traffic Class packet expansion scheduler policy is applied uniformly across the entire system.

Enter **no qos queue multicast scheduler** to return the multicast Traffic Class packet expansion scheduler to the default value.

Examples

To set the multicast Traffic Class packet expansion scheduler for Traffic Class 0 getting 5 percent bandwidth, Traffic Class 1 getting 10 percent bandwidth, Traffic Class 2 getting 15 percent bandwidth, and Traffic Class 3 getting 20 percent bandwidth, and so on:

```
switch(config)# qos queue multicast scheduler dwrr 5 10 15 20 5 10 15 20
```

To return the system to the default multicast Traffic Class packet expansion scheduler policy:

```
switch(config)# no qos queue multicast scheduler
```

Related Commands

qos rcv-queue multicast rate-limit

qos queue scheduler

Configures the Traffic Class packet scheduler policy.

Syntax

qos queue scheduler strict-priority *strict-priority-number* **dwrr** *weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7*

no qos queue scheduler

Command Default

The default strict priority value is 8. There is no default value for each weight value.

Parameters

strict-priority

Configures the Strict Priority Traffic Class policy. All Strict Priority Traffic Classes are serviced before any DWRR Traffic Classes.

strict-priority-number

Sets the number of the Strict Priority Traffic Class. This is the strict priority number of the highest Traffic Class. For example, if the strict priority number is 3, the Strict Priority Traffic Classes contains Traffic Classes 7, 6, and 5. Valid values range from 0 through 8.

dwrr

Configures the DWRR Traffic Class policy. There are a variable number of DWRR weight values accepted that are dependent on the setting of strict priority number. The strict priority number plus the number of DWRR weight values must always add up to 8 Traffic Classes.

weight0

Sets the DWRR weight for Traffic Class 0 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight0* value is only valid when the strict priority number is less than 8. Valid values range from 0 through 100 percent.

weight1

Sets the DWRR weight for Traffic Class 1 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight1* value is only valid when the strict priority number is less than 7. Valid values range from 0 through 100 percent.

weight2

Sets the DWRR weight for Traffic Class 2 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight2* value is only valid when the strict priority number is less than 6. Valid values range from 0 through 100 percent.

weight3

Sets the DWRR weight for Traffic Class 3 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight3* value is only valid when the strict priority number is less than 5. Valid values range from 0 through 100 percent.

weight4

Sets the DWRR weight for Traffic Class 4 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight4* value is only valid when the strict priority number is less than 4. Valid values range from 0 through 100 percent.

weight5

Sets the DWRR weight for Traffic Class 5 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight5* value is only valid when the strict priority number is less than 3. Valid values range from 0 through 100 percent.

weight6

Sets the DWRR weight for Traffic Class 6 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight6* value is only valid when the strict priority number is less than 2. Valid values range from 0 through 100 percent.

weight7

Sets the DWRR weight for Traffic Class 7 in units of bandwidth percentage left over after servicing all of the Strict Priority Traffic Classes. The sum of all weight values must equal 100 percent. The *weight7* value is only valid when the strict priority number is less than 1. Valid values range from 0 through 100 percent.

Modes

Global configuration mode

Usage Guidelines

Eight Traffic Classes are supported with a configurable number of them being Strict Priority and any remaining ones being serviced DWRR. This Traffic Class packet scheduler policy is applied uniformly across the entire system. Actual Traffic Class packet scheduling is performed independently by each switch.

In Brocade VCS Fabric mode, this command does not take effect and will result in a error. To update the scheduling, please use the CEE map configuration.

Enter **no qos queue scheduler** to return the Traffic Class packet scheduler to the default value.

Examples

To set the Traffic Class packet scheduler for four Strict Priority Traffic Class and four DWRR Traffic Class with Traffic Class 0 getting 10 percent bandwidth, Traffic Class 1 getting 20 percent bandwidth, Traffic Class 2 getting 30 percent bandwidth, and Traffic Class 3 getting 40 percent bandwidth:

```
switch(config)# qos queue scheduler strict-priority 4 dwrr 10 20 30 40
```

To return the system to the default Traffic Class packet scheduler policy:

```
switch(config)# no qos queue scheduler
```

Related Commands

qos rcv-queue multicast rate-limit, qos rcv-queue multicast threshold

qos random-detect traffic-class

Maps a Random Early Discard (RED) profile to a CoS priority value for a port.

Syntax

qos random-detect traffic-class *value* **red-profile-id** *profile-ID value*

no qos random-detect cos *value*

Command Default

Port CoS priority value is not mapped to the RED profile.

Parameters

value

Class of Service (COS) value. Valid values range from 0 through 7.

profile-ID value

Random Error Detection value. Valid values range from 1 through 384.

Modes

Interface subtype configuration mode

Usage Guidelines

The RED profile is defined by the **qos red-profile** command.

Enter **no qos random-detect cos** *value* while in the interface mode to remove the DSCP-to-Traffic-Class map from the interface.

Examples

To map the profile to CoS priority 7 on the 10-gigabit Ethernet interface 1/2/2:

```
switch(config)# interface tengigabitethernet 1/2/2
switch(conf-if-te-1/2/2)# qos random-detect cos 7 red-profile-id 2
```

To remove the previously created profile from interface 1/2/2:

```
switch(config)# interface tengigabitethernet 1/2/2
switch(conf-if-te-1/2/2)# no qos random-detect cos 7
```

Related Commands

interface, qos red profile, show qos red profiles, show qos red statistics interface

qos rcv-queue cos-threshold

Configures the port tail drop thresholds.

Syntax

qos rcv-queue cos-threshold *TDT0* { *TDT1* | *TDT2* | *TDT3* | *TDT4* | *TDT5* | *TDT6* | *TDT7* }

no qos rcv-queue cos-threshold

Parameters

TDT0
Defines the proportion for the first port tail drop threshold. Valid values range from 0 through 100.

TDT1
Defines the proportion for the second port tail drop threshold. Valid values range from 0 through 100.

TDT2
Defines the proportion for the third port tail drop threshold. Valid values range from 0 through 100.

TDT3
Defines the proportion for the fourth port tail drop threshold. Valid values range from 0 through 100.

TDT4
Defines the proportion for the fifth port tail drop threshold. Valid values range from 0 through 100.

TDT5
Defines the proportion for the sixth port tail drop threshold. Valid values range from 0 through 100.

TDT6
Defines the proportion for the seventh port tail drop threshold. Valid values range from 0 through 100.

TDT7
Defines the proportion for the eighth port tail drop threshold. Valid values range from 0 through 100.

Modes

Interface subconfiguration mode (gi, te).

Usage Guidelines

Every port has associated with it a total of nine CoS thresholds, one for the port tail drop threshold and the other eight are thresholds for per priority. To give a fair allocation of buffers for the traffic from all priorities, the port buffers are allocated among different priorities. That is achieved through per priority tail drop thresholds. The port tail drop threshold represents the amount of buffers given to the port and per priority tail drop thresholds (CoS tail drop thresholds from now on) represents the buffers allocated to each CoS.

Whenever the buffers allocated to a priority are fully exhausted, all the traffic coming in on that priority is dropped. In the absence of per priority tail drop thresholds (and only port tail drop threshold), the buffers would be consumed on a first come first serve basis and results in an unfair share of buffers between all the priorities.

If you know which priority traffic is most seen, then giving good number of buffers for those priorities results in less number of packet drops for those priorities. Therefore, instead of using the standard priority values, you can assign any priority from 0% to 100% to any threshold; however, the sum value of all eight priorities must not exceed 100%. For example, using the priorities 5 5 5 5 50 20 2 8 sums up to 100%.

The tail drop thresholds are not allowed to exceed 100%, but can be below 100%. For example, if the tail drop thresholds entered are less than 100%, then the buffer allocation happens as per what has been configured.

NOTE

Brocade recommends *not* configuring cos-thresholds on an edge interface for a COS value with pause/priority flow control enabled. Doing so could create buffer-allocation issues.

Enter **no qos rcv-queue cos-threshold** to remove the configured tail drop thresholds.

Examples

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos rcv-queue cos-threshold 5 5 5 5 50 20 2 8
switch(conf-if-te-178/0/9)# do show qos in te 178/0/9
Interface Ten Gigabit Ethernet 178/0/9
CoS-to-Traffic Class map 'default'
               In-CoS:   0   1   2   3   4   5   6   7
  ------------------------------------------------------
  Out-CoS/TrafficClass: 0/1 1/0 2/2 3/3 4/4 5/5 6/6 7/7
Per-Traffic Class Tail Drop Threshold (bytes)
         TC:      0      1      2      3      4      5      6      7
  ------------------------------------------------------------------
  Threshold:  10180  10180  10180  10180 101808  40723   4072  16289
```

Related Commands

interface, qos rcv-queue multicast threshold

qos rcv-queue limit

Controls high burst traffic received on the Brocade VDX 6740.

Syntax

qos rcv-queue limit { *buffering_upper_limit* }

Command Default

The default value is 283 KB.

Parameters

buffering_upper_limit

Defines the upper limit of buffering for the port. The range of queue limit values is from 128 KB through 8 MB. While any value within this range is valid, recommended values are 128, 256, 512, 1024, and 2048.

Modes

RBridge ID configuration mode

Usage Guidelines

With enhanced shared dynamic buffering mechanism, an interface is capable of bursting up to the recommended 2MB limit. Though a maximum of 8MB is allowed, you should consult your Brocade Engineer, as it may impact the performance of the other ports that may need to burst at the same time.

Examples

Typical command example:

```
switch(config-rbridge-1)# qos rcv-queue limit 8000
```

History

Release version	Command history
4.0.1	This command was introduced.

Related Commands

qos tx-queue limit

qos rcv-queue multicast rate-limit

Configures a cap on the maximum rate for multicast packet expansion such as packet replication. The rate limit is applied uniformly across the entire system and is enforced independently by each switch.

Syntax

qos rcv-queue multicast rate-limit *rate* [**burst** *burst-size*]

no qos rcv-queue multicast rate-limit

Command Default

The burst size is 4096 packets. The rate value is 3000000 pkt/s.

Parameters

rate

Specifies the maximum rate for multicast packet expansion in units of packets per second (pkt/s). Valid values range from 6500 through 20000000 pkt/s.

burst *burst-size*

Configures a cap on the maximum burst size for multicast packet expansion. Valid values range from 50 through 65535 packets.

Modes

Global configuration mode

Usage Guidelines

This command is not supported on VDX 8770-4 and VDX 8770-8 switches.

The *rate* parameter places a cap on the sum of the first level expansion (for example, the ingress packets replicated for each egress switch) plus the second level expansion (for example, packets replicated for egress interfaces on the switch).

The **burst** *burst-size* parameter represents the maximum number of multicast packet expansion that can be performed back-to-back as a single burst in units of packets (pkt).

Enter **no qos rcv-queue multicast rate-limit** to return the multicast packet expansion rate limit to the default settings.

Examples

To lower the maximum multicast packet expansion rate to 10000 pkt/s:

```
switch(config)# qos rcv-queue multicast rate-limit 10000
```

To return the system to the default multicast packet expansion rate limit values:

```
switch(config)# no qos rcv-queue multicast rate-limit
```

Related Commands

qos rcv-queue multicast threshold

qos rcv-queue multicast threshold

Configures a cap on the maximum queue depth for multicast packet expansion queues.

Syntax

qos rcv-queue multicast threshold *mTC0 mTC1 mTC2 mTC3 mTC4 mTC5 mTC6 mTC7*

no qos rcv-queue multicast threshold

Command Default

64 packets for each multicast Traffic Class.

Parameters

mTC0

Sets the Tail Drop Threshold for multicast Traffic Class 0 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC1

Sets the Tail Drop Threshold for multicast Traffic Class 1 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC2

Sets the Tail Drop Threshold for multicast Traffic Class 2 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC3

Sets the Tail Drop Threshold for multicast Traffic Class 3 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC4

Sets the Tail Drop Threshold for multicast Traffic Class 4 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC5

Sets the Tail Drop Threshold for multicast Traffic Class 5 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC6

Sets the Tail Drop Threshold for multicast Traffic Class 6 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

mTC7

Sets the Tail Drop Threshold for multicast Traffic Class 7 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

Modes

Global configuration mode

Usage Guidelines

The individual Tail Drop Threshold is specified for each of the four multicast traffic classes. These Tail Drop Thresholds are applied uniformly across the entire system. These queue depths are enforced independently by each switch.

This command is not supported on VDX 8770-4 and VDX 8770-8 switches.

Enter **no qos rcv-queue multicast threshold** to return the multicast expansion queues to the default value.

Examples

To increase multicast packet expansion Tail Drop Threshold to 1000 pkt for each multicast Traffic Class:

```
switch(config)# qos rcv-queue multicast threshold 1000 1000 1000 1000 1000 1000 1000 1000
```

To return the system to the default multicast packet expansion Tail Drop Threshold value:

```
switch(config)# no qos rcv-queue multicast threshold
```

Related Commands

qos rcv-queue multicast rate-limit

qos red profile

Creates a Random Early Discard (RED) profile for egress traffic flow and provides a minimum threshold, maximum threshold, and drop-probability for egress traffic flow.

Syntax

qos red-profile *profile-ID value* **min-threshold** *percentage* **max-threshold** *percentage* **drop-probability** *percentage*

no qos red-profile *profile-IDvalue*

Parameters

profile-ID value
Valid values range from 1 through 384.

percentage
0 through 100 percent.

min-threshold
Minimum threshold (percentage) of queue size (0 through 100) for randomly dropping packets.

max-threshold
Maximum threshold (percentage) of queue size (0 through 100) when packets are dropped with 100% probability.

drop-probability
Probability that packets will be dropped when minimum threshold is reached.

Modes

Global configuration mode

Usage Guidelines

Enter **qos random-detect cos** command while in configuration mode for a specific interface to map the profile to a CoS priority for a port.

Enter **no qos random-detect cos** command while in the interface mode to remove the profile from the interface. You must remove the profile from interface before you can remove the profile itself.

Enter **no qos red-profile** *profile-ID* to remove the profile while in global configuration mode.

NOTE
This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a RED profile while in global configuration mode:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# qos red-profile 2 min-threshold 10 max-threshold 80 drop-probability 80
```

To remove the profile while in global configuration mode:

```
switch(config)# no qos red-profile 2
```

Related Commands

show qos red profiles

qos service-policy

Activates the global service policy mode that allows you to apply a service policy to a single Rbridge ID, a range of Rbridge IDs, or all Rbridge IDs.

Syntax

qos service-policy { **in** | **out** } *service_policy_name*

Parameters

in
Applies the service policy to inbound traffic.

out
Applies the service policy to outbound traffic.

service_policy_name
The name of the service policy to apply to the Rbridge ID.

Modes

Global configuration mode

Examples

Example of applying a service policy to inbound traffic on all Rbridge IDs.

```
switch# configure terminal
switch(config)# qos service-policy in policymap1
switch(config-service-policy)# attach rbridge-id add all
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

attach rbridge-id, class, policy-map, show class-maps, show policymap

qos trust cos

Specifies the interface QoS trust Class of Service (CoS), which controls user priority mapping of incoming traffic.

Syntax

qos trust cos

no qos trust cos

Command Default

The QoS trust mode set to the untrusted state.

Modes

Interface subtype configuration mode

Usage Guidelines

The untrusted mode overrides all incoming priority markings with the Interface Default CoS. The CoS mode sets the user priority based on the incoming CoS value, if the incoming packet is not priority tagged, then fallback is to the Interface Default CoS value.

When a CEE map is applied on an interface, the **qos trust cos** command is not allowed. The CEE map always puts the interface in the CoS trust mode.

Enter **no qos trust cos** to return to the default.

Examples

To set the interface QoS to the CoS trust mode for a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos trust cos
```

To return the interface QoS to the default value or to the untrusted state:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no qos trust cos
```

When a CEE map is applied, the switch does not allow the **qos trust cos** command and displays the following error:

```
switch(conf-if-te-0/1)# cee demo
switch(conf-if-te-0/1)# qos trust cos
% Error: QoS is not in non-CEE Provisioning mode
```

Related Commands

interface, qos cos, show qos maps

qos trust dscp

Enables Differentiated Services Code Point (DSCP) which controls user priority mapping of incoming traffic

Syntax

qos trust dscp

no qos trust dscp

Command Default

The QoS trust DSCP mode set to the untrusted state.

Modes

Interface subtype configuration mode

Usage Guidelines

The untrusted mode overrides all incoming priority markings with the Interface Default CoS. The DSCP trust mode sets the user priority based on the incoming DSCP value, When this feature is not enabled, DSCP values in the packet are ignored.

When DSCP trust is enabled, the following lists the default mapping of DSCP values to user priority.

TABLE 12 Default DSCP priority mapping

DSCP Values	User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

QoS Trust Mode is automatically applied if **dscp-cos map** or **qos dscp traffic class** is applied to the interface.

Enter **no qos trust dscp** to return to the default.

Examples

To set the interface QoS to DCSP trust mode on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# qos trust dscp
```

To return the interface QoS to the default value or to the untrusted state:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no qos trust dscp
```

Related Commands

interface, qos map dscp-cos, qos map dscp-traffic-class, show qos interface, show qos maps dscp-traffic-class

qos tx-queue limit

Controls high burst traffic transmitted on the Brocade VDX 6740.

Syntax

qos tx-queue limit { *buffering_upper_limit* }

Command Default

The default value is 283 KB.

Parameters

buffering_upper_limit

Defines the upper limit of buffering for the port.
The range of queue limit values is from 128 KB through 8 MB. While any value within this range is valid, recommended values are 128, 256, 512, 1024, and 2048.

Modes

RBridge ID configuration mode

Usage Guidelines

With enhanced shared dynamic buffering mechanism, an interface is capable of bursting up to the recommended 2MB limit. Though a maximum of 8MB is allowed, you should consult your Brocade Engineer, as it may impact the performance of the other ports that may need to burst at the same time.

Examples

Typical command example:

```
switch(config-rbridge-1)# qos tx-queue limit 8000
```

History

Release version	Command history
4.0.1	This command was introduced.

Related Commands

qos rcv-queue limit

qos-profile (AMPP)

Activates the QoS profile mode for AMPP. This mode allows configuration of QoS attributes of a port-profile.

Syntax

qos-profile

no qos-profile

Modes

Port-profile configuration mode

Usage Guidelines

Enter **no qos-profile** to remove the profile.

Examples

```
switch(config)# port-profile sample-profile
switch(conf-pp)# qos-profile
```

radius-server

Configures the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

radius-server host { *ip-address* | *host_name* } [**auth-port** *portnum*] [**protocol** { **chap** | **pap** | **peap** }] [**key** *shared_secret*] [**encryption-level** *value_level*] [**timeout** *sec*] [**retries** *num*]

no radius-server host *hostname* | *ip-address*

Command Default

A Remote Authentication Dial-In User Service (RADIUS) server is not configured.

Parameters

host { *ipaddr* | *host_name* }

Specifies the IP address or host name of the RADIUS server. IPv4 and IPv6 addresses are supported. The maximum supported length for the RADIUS hostname is 40 characters.

auth-port *portnum*

Specifies the user datagram protocol (UDP) port used to connect the RADIUS server for authentication. The valid range is 0 through 65535. The default port is 1812.

protocol { **chap** | **pap** | **peap** }

Specifies the authentication protocol. Parameters include CHAP, PAP, or PEAP-MSCHAP. The default is CHAP.

key *shared_secret*

The text string that is used as the shared secret between the switch and the RADIUS server. The default is **sharedsecret** . The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the shared secret string in either double quotation marks or use the escape character (\). For example: **"secret!key"** or **secret\!key** .

encryption-level *value_level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

timeout *sec*

The time to wait for the RADIUS server to respond, in seconds. The default is 5 seconds.

retries *num*

The number of attempts allowed to connect to a RADIUS server. The default is 5 attempts.

Modes

Global configuration mode

Usage Guidelines

If a RADIUS server with the specified IP address or host name does not exist, it is added to the server list. If the RADIUS server already exists, this command modifies the configuration.

The **key** parameter does not support an empty string.

Enter **no radius-server** to reset to their default values.

NOTE
Before downgrading to a Network OS version that does not support the **encryption-level** keyword, set the value of this keyword to 0. Otherwise, the firmware download will throw an error that requests this value be set to 0.

Examples

To configure a RADIUS server:

```
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit 100
switch(config-radius-server-10.24.65.6)#
```

To modify the previously configured RADIUS server:

```
switch(config)# radius-server host 10.24.65.6 protocol pap key "new#radius*secret timeout 10
```

To reset the timeout value to the default:

```
switch(config)# no radius-server host 10.24.65.6 timeout
```

Related Commands

show running-config radius-server, show running-config tacacs-server, tacacs-server

rasman

Displays RASLog messages decoding and documentation on the switch.

Syntax

rasman [[**module-description**] | [**message id** *RAS-message-id*] | [**module type** *module-name*] | [**type value** *RAS-message-type*]]

Parameters

module-description
Displays the RAS module description.

message id *RAS-message-id*
Displays the RAS message ID details.

module type *module-name*
Displays the RAS message ID based on module. Displays all external RAS messages.

type value *RAS-message-type*
Displays the RAS message ID based on type. Possible completions: AUDIT, DCE, FFDC, LOG, and VCS.

Modes

Privileged EXEC mode

Usage Guidelines

Input value is case-sensitive.

Examples

To display the module descriptions:

```
sw0# rasman module-description
RASModule      ID       Description
-----------------------------------------------------
KT             1        Kernel Test ID
UT             2        User Test ID
TRCE           3        Trace Subsystem (User)
KTRC           4        Trace Subsystem (Kernel)
LOG            5        RASLOG module
CDR            6        Condor ASIC driver
```

To display the messages pertaining to the AUTH module:

```
sw0# rasman module type AUTH
RAS Message ID     Severity    Message
-------------------------------------------------------
AUTH-1001          INFO        %s has been successfully completed.
AUTH-1002          ERROR       %s has failed.
AUTH-1003          INFO        %s type has been successfully set t
AUTH-1004          ERROR       Failed to set %s type to %s.
AUTH-1005          ERROR       Authentication file does not exist:
AUTH-1006          WARNING     Failed to open authentication confi
AUTH-1007          ERROR       The proposed authentication protoco
AUTH-1008          ERROR       No security license, operation fail
```

To display the AUDIT messages.

```
sw0# rasman type value AUDIT
RAS Message ID     Severity     Message
-----------------------------------------------------------------
FCIP-1002          INFO        An IPsec/IKE policy was added
FCIP-1003          INFO        An IPsec/IKE policy was deleted
AUTH-1045          ERROR       Certificate not present in this switch
AUTH-1046          INFO        %s has been successfully completed
AUTH-1047          ERROR       %s has failed
AUTH-3001          INFO        Event: %s, Status: success, Info: %
AUTH-3002          INFO        Event: %s, Status: success, Info: %
```

Example of rasman type value DCE.

```
sw0# rasman type value DCE
RAS Message ID Severity Message
-------------------------------------------------
LACP-1001 ERROR %s Error opening socket (%d)
LACP-1002 ERROR %s %s
LACP-1003 INFO Port-channel %d up in defaulted state
LACP-1004 INFO Port-channel %d down from default
NSM-1001 INFO Interface %s is online
NSM-1002 INFO Interface %s is protocol down
```

Example of rasman type value LOG:

```
sw0# rasman type value LOG
RAS Message ID Severity Message
-----------------------------------------------------------------------
FCIP-1000 ERROR %s of GE %d failed. Please retry
FCIP-1001 CRITICAL FIPS %s failed; algo=%d type=%d slot
FCIP-1002 INFO An IPsec/IKE policy was added
FCIP-1003 INFO An IPsec/IKE policy was deleted
FCIP-1004 INFO Tape Read Pipelining is being disabled
AUTH-1001 INFO %s has been successfully completed
AUTH-1002 ERROR %s has failed
```

Example of rasman type value VCS:

```
sw0# rasman type value VCS
RAS Message ID Severity Message
-----------------------------------------------------------------------
SS-2000 INFO Copy support started on rbridge-id
SS-2001 INFO Copy support completed on rbridge-id
SS-2002 INFO Copy support failed on rbridge-id %
SULB-1105 WARNING Firmware upgrade session (%d: %s) s
SULB-1106 WARNING Firmware upgrade session (%d: %s) c
SULB-1107 WARNING Firmware upgrade session (%d: %s) f
```

rate-limit-delay get netconf

Returns the rate limit delay configured for processing NETCONF Remote Procedure Calls (RPCs).

Syntax

rate-limit-delay get netconf

Modes

Privileged EXEC mode

Usage Guidelines

This command returns the configured minimum time in milliseconds between processing successive NETCONF RPCs. A value of 0 indicates that RPC processing is unlimited.

Related Commands

rate-limit-delay set netconf

rate-limit-delay set netconf

Limits the rate at which BNA or NETCONF Remote Procedure Call (RPC) requests can be processed on the switch.
Synopsisrate-limit-delay set netconf delay

Syntax

rate-limit-delay set netconf *value*

Command Default

The default is 0.

Parameters

value

The number of milliseconds the system waits between processing RPCs.

Modes

Privileged EXEC mode

Usage Guidelines

The rate at which RPCs can be processed on the switch is specified the minimum delay between processing successive RPCs. The default of 0 means that the RPC processing rate is unlimited.

Use this command to prevent excessive numbers of RPCs from adversely affecting switch performance.

Examples

This example limits the processing of RPCs to a maximum of one every 50 milliseconds.

```
switch# debug internal rate-limit-delay set netconf 50
```

Related Commands

rate-limit-delay get netconf

rbridge-id

Enables RBridge ID configuration mode to support VCS on individual nodes.

Syntax

rbridge-id *rbridge-id*

no rbridge-id *rbridge-id*

Parameters

rbridge-id

The number of an RBridge node.

Modes

Global configuration mode

Usage Guidelines

Use this command to enter RBridge ID configuration mode for fabric cluster and logical chassis cluster configuration.

CAUTION

It is always preferable to have the RBridge ID configured on a switch. If the RBridge ID is not configured, deleting the interface IP address that matches the router ID will cause an OSPF process reset and a spike in CPU usage.

Examples

Use the**rbridge-id ?** command in global configuration mode to see available nodes.

Enter RBridge ID configuration mode and use ? to view commands available in that mode:

```
sw0(config)# rbridge-id 154
sw0(config-rbridge-id-154)# ?
Possible completions:
  arp                           Address Resolution Protocol (ARP)
  chassis
  do                            Run an operational-mode command
  exit                          Exit from current mode
  fabric                        Allows to configure fabric related parameters
  fcsp                          FCSP configuration commands
  filter-change-update-delay    Change filter change update delay timer
  help                          Provide help information
  interface                     Interface configuration
  ip                            Configure Internet Protocol (IP)
  ipv6                          Configure Internet Protocol (IPv6)
  logical-chassis               Logical chassis commands
  management                    The list of management interfaces.
  no                            Negate a command or set its defaults
  protocol                      Protocol configuration
  pwd                           Display current mode path
  route-map                     Configure a route-map instance
  router                        Configure router
  secpolicy                     Security policy related configuration
  ssh                               Configure SSH Server
  switch-attributes             Switch attributes configurations
  system-monitor                Configure FRU threshold and alert setting
  telnet                        Configure Telnet Server
  threshold-monitor             Configure Class monitoring threshold and alert
                                setting
  top                           Exit to top level and optionally run command
  vrf                           VRF configurations
```

rd (route distinguisher)

Distinguishes a route for VRF.

Syntax

rd *admin-value*:*arbitrary-value*

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.

Modes

VRF configuration mode

Usage Guidelines

This command allows you to use the same IP address in different VPNs without creating any conflicts. The Route Distinguisher parameter can be either ASN-relative or IP address-relative.

Once the Route Distinguisher is configured for a VRF it cannot be changed or deleted.

To remove the Route Distinguisher, you must delete the VRF.

Examples

To configure Route Distinguisher:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rbridge-id 53
switch(config-rbridge-id-53)# vrf red
switch(config-vrf-red)# rd 101:101
```

To remove Route Distinguisher, remove the VRF.

```
switch(config-vrf-red)# no vrf red
```

Related Commands

vrf, ip router-id

reconnect-interval

Sets the reconnect interval between the NSX controller and the VCS fabric.

Syntax

reconnect-interval *interval*

no reconnect-interval

Command Default

10 seconds

Parameters

interval

Specifies the maximum number of seconds to wait between connection attempts. Value must be in the range of 1 to 1000.

Modes

NSX controller configuration mode

Usage Guidelines

Use this command to set the reconnect interval for the NSX controller connection profile. If the connection is lost between the NSX and the VCS fabric, a reconnection attempt occurs at this interval.

This command is allowed for a switch that is in logical chassis cluster mode only.

Use the **no** form of the command to revert the reconnect interval to the default value.

Examples

To set the reconnect interval to 30 seconds for an NSX controller profile that you have already created (named *profile1)* :

```
switch# configuration
switch(config)# nsx-controller profile1
switch(config-nsx-controller-profile1)# reconnect-interval 30
```

redistribute (BGP)

Configures the device to redistribute OSPF, ISIS, or RIP routes, directly connected routes, or static routes into BGP4 and BGP4+.

Syntax

redistribute { **connected** | **static** } [**metric** *num* | **route-map** *string*]

no redistribute { **connected** | **static** } [**metric** *num* | **route-map** *string*]

Command Default

The device does not redistribute routing information between BGP4 or BGp4+ and the IP interior gateway protocol OSPF.

Parameters

connected
Redistributes connected routes.

static
Redistributes static routes.

metric
Metric for redistributed routes.

num
Specifies a metric number. The range is from 0 through 4294967297. No value is assigned by default.

route-map
Specifies that a route map be consulted before a route is added to the routing table.

string
Specifies a route map to be consulted before a route is added to the routing table.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command to configure the device to redistribute OSPF, directly connected routes, or static routes into BGP4 or BGP4+. The routes can be filtered by means of an associated route map before they are distributed.

Use the **no** form of the command to restore the defaults.

NOTE
The **default-metric** command does not apply to the redistribution of directly connected routes into BGP4 or BGP4+. Use a route map to change the default metric for directly connected routes.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# redistribute static metric 200
```

To redistribute directly connected routes into BGP4+ and specify route-map 5 to be consulted.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv6 unicast
switch(config-bgp-ipv6u)# redistribute static metric 200
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map, default-metric (OSPF)

redistribute (OSPF)

Configures the device to redistribute OSPF routes.

Syntax

redistribute ospf { **match** [**external1** | **external2** | **internal**] } [**metric** *num*] | **route-map** *string*

no redistribute ospf { **match** [**external1** | **external2** | **internal**] } [**metric** *num*] | **route-map** *string*

Command Default

Internal OSPF routes are distributed. No value is assigned for *num* .

Parameters

match
Selects the type of route to be redistributed.

external1
Redistributes OSPF external type 1 routes.

external2
Redistributes OSPF external type 2 routes.

internal
Redistributes OSPF internal routes.

num
A value that assigns the metric.The range is from 0 through 4294967297.

string
Specifies a route map to be consulted before an OSPF route is added to the BGP4 routing table.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **redistribute ospf** command to redistribute all OSPF routes (OSPF external type 1, external type 2, or internal routes).
Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# redistribute ospf match external1 metric 200
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

default-metric (OSPF)

region

Assigns a name to the Multiple Spanning Tree Protocol (MSTP) region.

Syntax

region *region-name*

no region

Parameters

region-name

Assigns a name to an MSTP region.

Modes

Protocol Spanning Tree MSTP configuration mode

Usage Guidelines

The *region-name* string must be between 1 and 32 ASCII characters in length, and is case-sensitive.

If MSTP is enabled over VCS, this command must be executed on all RBridge nodes

Enter **no region** to delete the region name.

Examples

To assign a name to an MSTP region named brocade1:

```
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# region brocade1
```

Related Commands

revision, show spanning-tree

reload

Reboots the control processor (CP) or management module (MM).

Syntax

reload [**standby** | **system**]

reload system [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

standby

Reboots the standby CP or MM on a dual CP/MM chassis.

system

Reboots an entire chassis.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This command performs a "cold reboot" (power off and restart) of the CP or MM.

The **reload** operation is generally disruptive and the command prompts for confirmation before executing. When you reboot a switch connected to a fabric, all traffic to and from that switch stops. All ports on that switch remain inactive until the switch comes back online.

On a Top-of-Rack (ToR) switch, If the power-on-self-test (POST) is enabled, it is executed when the system comes back up.

On a modular chassis, the **reload** commands only reboots the management module on which the command is executed. If you log in to the switch IP address and execute the **reload** command, only the active management module reboots and POST is bypassed.

The available modes are listed below.

TABLE 13 Available modes

Mode	Definition
Standalone	Standalone. A node is in Standalone mode when Virtual Cluster Switching (VCS) is disabled.

TABLE 13 Available modes (continued)

FC	Fabric cluster. In FC mode, the data path for nodes is distributed, but the configuration path is not distributed. Each node maintains its own configuration database.
LC	Logical chassis cluster. In LC mode, both the data path and the configuration path are distributed.

The following summarizes the behavior of the **reload** command under a variety of conditions.

TABLE 14 Behavior of the **reload** command

Command	HA synchronized		HA not synchronized	
	Active	Standby	Active	Standby
reload	If executed on active MM, reboots that MM 1.	If executed on active MM, reboots that MM.	The user is prompted to execute the **reload system** command.	N/A
	In FC mode, the running configuration becomes the new active configuration.			N/A
	In LC mode, the running configuration becomes the new active configuration.			N/A
reload standby	Reboots the standby MM.	Reboots the standby MM.	Reboots the standby MM.	Reboots the standby MM.
reload system	Reboots the chassis and remains the master MM.	Not allowed.	If executed on active MM, reboots the chassis and remains the master MM.	Not allowed.
	In FC mode, the startup configuration is used.		In FC mode, the startup configuration is used.	
	In LC mode, the running configuration is used.		In LC mode, the running configuration is used.	

Examples

To perform a cold reboot on the switch:

```
switch# reload

Warning: Unsaved configuration will be lost. Please run `copy running-config startup-config` to save
the current configuration if not done already.
Are you sure you want to reload the switch [y/n]?: y
```

Related Commands

fastboot, ha chassisreboot, ha failover

remap fabric-priority

Remaps the CoS fabric priority to a different priority for Brocade VCS Fabric mode.

Syntax

remap fabric-priority *priority*

Command Default

The default is 0.

Parameters

priority

Specifies the remapped CoS priority value for Brocade VCS Fabric mode. The valid range is 0 through 6.

Modes

CEE map configuration mode

remap lossless-priority

Remaps the Brocade VCS Fabric Fabric lossless priorities to a different priority

Syntax

remap lossless-priority *priority*

Parameters

priority

Specifies the remapped priority value. Valid values range from 0 through 6. Default is 0.

Modes

CEE map configuration mode

rename

Renames a file in the switch flash memory.

Syntax

rename *current_name new_name*

Parameters

current_name
The file name you want to change.

new_name
The new file name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

System files cannot be renamed. If you try to rename a system file, a warning message is displayed.

Examples

To rename a file:

```
switch# rename myconfig.vcs myconfig.old

switch# dir

total 24
drwxr-xr-x   2 root     sys          4096 Feb 13 00:39 .
drwxr-xr-x   3 root     root         4096 Jan  1  1970 ..
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 myconfig.old
-rwxr-xr-x   1 root     sys           417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys           697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root         6800 Feb 13 00:37 startup-config
```

Related Commands

copy, delete, dir, show file

rename (Access Gateway mode)

Provides a name for a port group or renames a port group in Access Gateway mode.

Syntax

rename *pg_name*

Parameters

pg_name
Port group name

Modes

Port Grouping configuration mode

Usage Guidelines

You must be in Port Grouping configuration mode for the specific port group to use this command. The *pg_name* cannot exceed 64 characters,.

Examples

Renaming port group pg-1 to pg-array24.

```
sw0(config-rbridge-id-3-ag-pg-1)# rename pg-array24
```

Related Commands

pg, show ag pg

resequence access-list

Reassigns sequence numbers to entries of an existing MAC,IPv4, or IPv6 access ist.

Syntax

resequence access-list { **ip** | **ipv6** | **mac** } *name seq_num increment*

Parameters

ip | **ipv6** | **mac**

Specifies the Layer 2 or Layer 3 ACL bound to an interface.

name

Specifies the name of a standard or an extended ACL. A maximum of 63 characters is allowed.

seq_num

Specifies the starting sequence number in the ACL. Valid values range from 1 through 4294967290.

increment

Specifies a value to increment the sequence number between rules. Valid values range from 1 through 4294967290.

Modes

Privileged EXEC mode

Usage Guidelines

Reordering the sequence numbers is useful when you need to insert rules into an existing ACL and there are not enough sequence numbers available. When all sequence numbers between rules are exhausted, this feature allows the reassigning of new sequence numbers to entries of an existing access list.Examples

To reorder the rules in a MAC ACL:

```
switch# show running-config access-list mac test

!
mac access-list standard test
 seq 1 permit 0011.2222.3333
 seq 2 permit 0011.2222.4444
 seq 3 permit 0011.2222.5555
 seq 4 deny 0011.2222.6666
!
switch# resequence access-list mac test 10 10

switch# show running-config access-list mac test

!
mac access-list standard test
 seq 10 permit 0011.2222.3333
 seq 20 permit 0011.2222.4444
 seq 30 permit 0011.2222.5555
 seq 40 deny 0011.2222.6666
!
```

To reorder the rules in an IPv6 ACL:

```
switch# show running-config ipv6 access-list distList

!
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any!
switch# resequence access-list ipv6 distList 100 100
switch# show running-config ipv6 access-list distList

!
ipv6 access-list standard distList
 seq 100 deny 2001:125:132:35::/64
 seq 200 deny 2001:54:131::/64
 seq 300 deny 2001:5409:2004::/64
 seq 400 permit any
!
```

Related Commands

mac access-list extended, seq (MAC extended ACLs), seq (IPv6 standard ACLs), seq (MAC standard ACLs)

reserved-vlan

Defines the range of 802.1Q VLANs that cannot be created by means of the **interface vlan** command.

Syntax

reserved-vlan *start-VLAN-ID end-VLAN-ID*

Command Default

VLANs 4087 through 4095 are reserved on the switch.

Parameters

start-VLAN-ID
Valid values range from1 through 4086.

end-VLAN-ID
Valid values range from 1 through 4086.

Modes

Global configuration mode

Usage Guidelines

NOTE
This command does not apply to service or transport VFs in a Virtual Fabrics context (VLAN ID > 4095).

The end value must be greater than the start value. This command succeeds if there are no VLANs configured in the specified range. Otherwise, an error instructs you to delete the configured VLANs in the specified range, or provide a different range.

VLAN 1002 is still the default FCoE VLAN. VLAN 1002 cannot be part of the reserved VLAN range unless some other VLAN is created for FCoE.

This command does not require a switch reboot.

Related Commands

show default-vlan, interface vlan, show running reserved-vlan

restrict-flooding

Restricts the flooding of egress BUM traffic from an AMPP port-profile port.

Syntax

restrict-flooding

no restrict-flooding

Command Default

Egress BUM traffic is allowed

Modes

Port-profile configuration mode

Usage Guidelines

This command is applicable only on the default profile and automatically applied to all the AMPP port-profile-ports on the switch.

This command only blocks the egress BUM traffic. Ingress traffic, known as unicast traffic, is not impacted.

Use the **no restrict-flooding** version of this command to remove the restriction.

Related Commands

fcoe-profile (AMPP), security-profile (AMPP), switchport, port-profile-port, port-profile (global configuration mode)

revision

Assigns a version number to the Multiple Spanning Tree Protocol (MSTP) configuration.

Syntax

revision *number*

no revision

Command Default

The default is 0.

Parameters

number

Specifies the revision or version number of the MSTP region. Valid values range from 0 through 255.

Modes

Protocol Spanning Tree MSTP configuration mode

Usage Guidelines

If MSTP is enabled over VCS, this command must be executed on all RBridges.

Enter **no revision** to return to the default setting.

Examples

To set the configuration revision to 1:

```
switch(config)# protocol spanning-tree mstp
switch(conf-mstp)# revision 1
```

Related Commands

region, show spanning-tree

rfc1583-compatibility (OSPF)

Configures compatibility with RFC 1583.

Syntax

rfc1583-compatibility

no rfc1583-compatibility

Command Default

OSPF is compatible with RFC 1583 (OSPFv2).

Modes

OSPF VRF router configuration mode

Usage Guidelines

OSPF is compatible with RFC 1583 (OSPFv2) and maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table. Disabling this compatibility causes the OSPF routing table to maintain multiple intra-AS paths, which helps prevent routing loops.

Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583.

Examples

To disable compatibility with RFC 1583:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# rfc1583-compatibility
```

rfc1587-compatibility (OSPF)

Configures compatibility with RFC 1587.

Syntax

rfc1587-compatibility

no rfc1587-compatibility

Command Default

OSPF is compatible with RFC 1587 (OSPFv2).

Modes

OSPF VRF router configuration mode

Usage Guidelines

RFC 1587is the original NSSA specification. Only part of the newer RFC 3101 is supported—the "no-summary" parameter and the handling of default-route LSAs when "no summary" is enabled.

Enter **no rfc1587-compatibility** to disable compatibility with RFC 1587.

Examples

To disable compatibility with RFC 1587:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# no rfc1587-compatibility
```

rib-route-limit (BGP)

Limits the maximum number of BGP Routing Information Base (RIB) routes that can be installed in the Routing Table Manager (RTM).

Syntax

rib-route-limit *num*

no rib-route-limit *num*

Command Default

This option is disabled. There is no limit.

Parameters

num

Decimal value for maximum number of RIB routes to be installed in the RTM. Range is from 1 through 65535.

Modes

BGP Address-Family IPv4 Unicast configuration mode

BGP Address-Family IPv6 Unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Beginning with Network OS v5.0.0, the **rib-route-limit** command controls the number of routes installed by BGP, irrespective of whether those BGP routes are the preferred routes in the system. BGP locally tracks the number of routes installed and the number of routes withdrawn from RIB. If the total number of routes installed exceeds the specified rib-route-limit, routes will not be installed.

If the rib-route-limit value is increased, route calculation is automatically triggered.

If the rib-route-limit value is decreased, you will be prompted to clear the BGP RTM.

Examples

To configure the device to limit the maximum number of BGP RIB routes that can be installed in the RTM:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# rib-route-limit 10000
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family and to control the number of routes installed by BGP.

rmon alarm

Sets the RMON alarm conditions.

Syntax

rmon alarm *index snmp_oid* **interval** *seconds* [**absolute** | **delta**] **rising-threshold** *value* **event** *number* [**falling-threshold** *value* **event** *number* [**owner** *name*]

no rmon alarm

Command Default

No alarms are configured.

Parameters

index
Specifies the RMON alarm index. Valid values range from 1 through 65535.

snmp_oid
Specifies the MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.16.1.1.1.5.65535. The object type must be a counter32.

interval *seconds*
Specifies the RMON alarm sample interval in seconds. Valid values range from 1 through 2147483648.

absolute
Sets the sample type as absolute.

delta
Sets the sample type as delta.

rising-threshold *value*
Specifies the RMON alarm rising threshold. Valid values range from 0 through 4294967295.

event *number*
Specifies the event for the rising alarm. Valid values range from 1 through 65535.

falling-threshold *value*
Specifies the RMON alarm falling threshold. Valid values range from 0 through 4294967295.

event *number*
Specifies the event for the rising alarm. Valid values range from 1 through 65535.

owner *name*
Specifies the identity of the owner. The maximum number of characters is 32.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon alarm** to disable the alarm conditions.

Examples

To set RMON alarm conditions:

```
switch(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.65535 interval 5 absolute rising-threshold 10000
event 100 falling-threshold 1000 event 101 owner admin
```

Related Commands

rmon event, show rmon

rmon collection history

Collects Ethernet group statistics for later retrieval.

Syntax

rmon collection history *number* [**buckets** *bucket_number* | **interval** *seconds* | **owner** *name*]

no romn collection history *number*

Command Default

RMON history collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

buckets *bucket_number*

Specifies the maximum number of buckets for the RMON collection history. Valid values range from 1 through 65535.

interval *seconds*

Specifies the alarm sample interval in seconds. Valid values range from 1 through 3600. The default value is 1800.

owner *name*

Specifies the identity of the owner. The maximum number of characters is 15.

Modes

Interface subtype configuration mode

Usage Guidelines

This command collects periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Enter **no rmon collection history** *number* to disable the history of statistics collection.

NOTE

RMON configuration is not supported on breakout ports in Network OS versions prior to v6.0.0.

Examples

To collect RMON statistics, with an RMON collection control index value of 5 for the owner named *admin* , on a specific 10-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface tengigabitethernet 170/0/1
device(conf-if-te-170/0/1)# rmon collection history 5 owner admin
```

Related Commands

interface, show rmon history

rmon collection stats

Collects Ethernet group statistics n a specific interface.

Syntax

rmon collection stats *number* [**owner** *name*]

no rmon collection stats *number*

Command Default

RMON statistic collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

owner *name*

Specifies the identity of the owner.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no rmon collection stats** *number* to disable the collection of statistics.

Ethernet group statistics collection is not supported on ISL links.

NOTE

RMON configuration is not supported on breakout ports in Network OS versions prior to v6.0.0.

Examples

To collect RMON statistics, with an RMON collection control index value of 2 for the owner named *admin* , on a specific 10-gigabit Ethernet interface:

```
device# configure terminal
device(config)# interface tengigabitethernet 170/0/1
device(conf-if-te-170/0/1)# rmon collection stats 2 owner admin
```

Related Commands

interface, show rmon history

rmon event

Adds or removes an event in the RMON event table associated to the RMON alarm number.

Syntax

rmon event *index* [**description** *word* | **log** | **owner** *name* | **trap** *word*]

no rmon event

Command Default

No events are configured.

Parameters

index
Specifies the RMON event number. Valid values range from 1 through 65535.

description *word*
Specifies a description of the event.

log
Generates an RMON log when an event is triggered.

owner *name*
Specifies the owner of the event. The *name* string must be between 1 and 32 characters in length.

trap *word*
Specifies the SNMP community or string name to identify this trap.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon event** to remove the event configuration.

Examples

To configure an RMON event:

```
switch(config)# rmon event 2 log description "My Errorstoday" owner gjack
```

Related Commands

show rmon history

role name

Creates or modifies a user role.

Syntax

role name *role_name* [**desc** *description*]

no role name

Parameters

role_name
The name of the role.

desc *description*
An optional description of the role.

Modes

Global configuration mode

Usage Guidelines

A role defines the access privileges of the user accounts on the switch. A user is associated with a single role. You first create the role and later associate the role with rules to define the access permissions.

The role name must begin with a letter and can contain alphanumeric characters and underscores. The length of the role name should be between 4 and 32 characters. The name cannot be same as that of an existing user.

The description field supports up to 64 characters and can include any printable ASCII character, except for the following characters: single quotation mark (‘), double quotation mark (“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces. you must enclose the text in double quotation marks.

The maximum number of roles supported is 64.

Enter **no role name** to set the attributes to their default values.

Examples

To create a role of a VCS administrator

```
switch(config)# role name VCSAdmin desc "Manages VCS fabrics"
```

To reset the description to the default value (no description):

```
switch(config)# no role name VCSAdmin desc
```

To delete the role:

```
switch(config)# no role name
```

Related Commands

rule, show running-config role, show running-config rule

root access console

Restricts the root access to the device to the console only.

Syntax

root access console

no root access console

Modes

RBridge ID configuration mode

Usage Guidelines

The **no root access console** allows root access to the device through all terminals (SSH, Telnet, and console).

Examples

Typical command output:

```
switch(config-rbridge-id-1)# do show running-config rbridge-id | include root
% No entries found.
switch(config-rbridge-id-1)# root access console
switch(config-rbridge-id-1)# do show running-config rbridge-id | include root
root access console
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

root enable

root enable

Enables root access to the device following a firmware configuration.

Syntax

root enable

no root enable

Modes

RBridge ID configuration mode

Usage Guidelines

The **no root enable** command disables root access to the device.

Examples

Typical command output:

```
switch(config-rbridge-id-1)# do show running-config rbridge-id | include root
% No entries found.
switch(config-rbridge-id-1)# root enable
% Info: Root password is at system default, for better security, you may want to change it.
switch(config-rbridge-id-1)# do show running-config rbridge-id | include root
root enable
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

root access console

route-map

Creates or deletes a route map instance, with a variety of options.

Syntax

route-map *name* [**permit** | **deny**] *instance_number* | [**continue** *sequence_number*]

no route-map *name* [**permit** | **deny**] *instance_number* | [**continue** *sequence_number*]

Parameters

name

The name of the route map. The string must be between 1 and 63 ASCII characters in length.

permit

Allows a matching pattern

deny

Disallows a matching pattern.

instance_number

The instance ID. The range is from 1 through 65535.

continue

Use a "continue" clause to allow for more programmable policy configuration and route filtering, with capability to execute additional entries in a route map after an entry is executed with successful "match" and "set" clauses.

sequence_number

The sequence ID. The range is from 1 through 65535.

Modes

RBridge ID configuration mode

Usage Guidelines

This command is used in conjunction with the on **match** and **set** commands. For details on these commands, refer to the Related Commands section:.

The maximum number of OSPF networks that can be advertised and processed in a single area in a router is limited to 600.

Enter **no route-map** *name* to remove the route-map name.

Related Commands

match (route map), match access-list, match as-path, match community, match interface, match ip address, match ip next-hop, match metric, match protocol bgp, match route-type, match tag, set as-path, set as-path prepend, set automatic-tag, set comm-list, set community, set cos traffic-class, set dscp, set dampening, set distance, set local-preference, set metric, set metric-type, set origin, set route-type, set tag, set weight

router bgp

Enables BGP4 and BGP4+ routing.

Syntax

router bgp

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no** form of this command to disable BGP4 routing.

Examples

To enable BGP4 routing:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)#
```

router ospf

Enables and configures the Open Shortest Path First (OSPF) routing protocol over virtual forward and routing (VRF) and enter OSPF VRF router configuration mode.

Syntax

router ospf [**vrf** *name*]

no router ospf

Command Default

Enabled

Parameters

vrf *name*

The name of the non-default VRF to connect.

Modes

RBridge ID configuration mode

Usage Guidelines

With Network OS4.0 and later OSPF can run over multiple Virtual Forwarding and Routing (VRF) mechanisms. OSPF maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

Enter **no router ospf** to delete all current OSPF configuration and to block any further OSPF configuration.

Examples

To enable OSPF on a default VRF and to enter OSPF VRF router configuration mode, run the **router ospf** command in RBridge ID configuration mode, as shown in the following example:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)
```

To enable OSPF on a non-default VRF and to enter OSPF VRF router configuration mode, run the **router ospf vrf** *name* command in RBridge ID configuration mode, as shown in the following example:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf vrf vrfname
switch(config-router-ospf-vrf-vrfname)
```

router pim

Enables or disables the Protocol Independent Multicast (PIM) routing protocol.

Syntax

router pim

no router pim

Command Default

The PIM protocol is disabled.

Modes

RBridge ID configuration mode

Usage Guidelines

This command launches the PIM router configuration mode.

Enter **exit** to exit this mode.

Examples

To enable the PIM protocol:

```
switch(config-rbridge-id-128)# router pim
```

route-target

Imports or exports the routes for the router-id for as pecified VRF.

Syntax

route-target [*admin-value*:*arbitrary-value*] [**export** | **import**]

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2 byte (from 0 through 65535) or a 4 byte number from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.

export

Exports the routes.

import

Import the routes.

Modes

VRF configuration mode

Related Commands

vrf

rp-address

Adds or removes a static rendezvous point address for a PIM domain.

Syntax

rp-address *A.B.C.D*

no rp-address

Command Default

No interface is configured as the rendezvous point candidate.

Parameters

A.B.C.D

The IP address that should be designated as the rendezvous point router.

Modes

PIM router configuration mode

Usage Guidelines

Since prefix-lists are not supported, the address is assumed to be the rendezvous point for 224.0.0.0/4 address range.

Enter **no rp-address** to disable this feature.

Examples

Setting the IP address to 12.12.12.12.

```
switch(conf-pim-router)# rp-address 12.12.12.12
```

Related Commands

router pim

rspan-vlan

Configures the VLAN to support RSPAN (Remote Switched Port Analyzer) traffic analysis.

Syntax

rspan-vlan

Modes

Interface subtype configuration mode

Usage Guidelines

RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network.

All participating switches must be trunk-connected at Layer 2, and RSPAN must be configured on all the switches participating in the RSPAN session.

Examples

Typical execution of this command.

```
switch(config)# interface vlan 300
switch(config-vlan-300)# rspan-vlan
```

Related Commands

interface vlan, show vlan

rule

Creates the Role-Based Access Permissions (RBAC) permissions associated with a role.

Syntax

rule *index* [**action** { **accept** | **reject** }] [**operation** { **read-only** | **read-write** }] **role** *role_name* **command** *command_name*

no rule *index*

Command Default

The default for **action** is **accept**. The default for **operation** is **read-write**.

Parameters

index
Specifies a numeric identifier for the rule. Valid values range from 1 through 512.

action accept | **reject**
Specifies whether the user is accepted or rejected while attempting to execute the specified command. The default value is **accept**.

operation read-only | **read-write**
Specifies the type of operation permitted. The default value is **read-write**.

role *role_name*
Specifies the name of the role for which the rule is defined.

command *command_name*
Specifies the command for which access is defined. Separate commands with a space. RBAC support is provided only for the following commands with parameters: copy, clear, interface, and protocol.

Modes

Global configuration mode

Usage Guidelines

Network OS uses RBAC as the authorization mechanism. Every user account must be associated with a role. Every user account can only be associated with a single role. Note that the permissions cannot be assigned directly to the user accounts and can only be acquired through the associated role.

When you create a rule, the **role**, *index*, and **command** operands are mandatory and the **action** and **operation** operands are optional. The maximum number of rules is 512.

When you modify a rule, all operands except *index* are optional.

Enter **no rule** *index* to remove the specified rule.

Examples

To create a rule allowing the NetworkSecurityAdmin role to create user accounts:

```
switch(config)# rule 150 action accept operation read-write role NetworkSecurityAdmin command config
switch(config)# rule 155 action accept operation read-write role NetworkSecurityAdmin command username
```

To delete a rule:

```
switch(config)# no rule 155
```

Related Commands

role name, show running-config role, show running-config rule

scheduler

Specifies the scheduling attributes along with the TC shape rate.

Syntax

scheduler *sp_count* [*shape_rate* | [*shape_rate* **...** *shape_rate*] **dwrr** [*weight* | *weight* **...** *weight*]

Parameters

sp_count

Specifies how many strict priority queues for each port scheduler. The range of valid values is from 0 through 8.

shape_rate

Specifies the shape rate on strict priority queues. The range of valid values are from 28000 kbps to the maximum interface speed.

dwrr *weight*

Specifies the dwrr weight percentage for the queue. The range of valid values is from 1% through 100%, and the sum of all dwrr weights should not exceed 100%.

Modes

Policy-map configuration mode

Usage Guidelines

There are total eight queues are present on an interface. The number of dwrr queues present depends on the SP_COUNT value. For example if the SP_COUNT is two, then there are two strict priority queues and six dwrr queues.

This command is allowed only for the Egress direction.

This command can only be configured in for the **class class-default** command.

This command is mutually exclusive of the **port-shape** and **police** commands.

Examples

Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# scheduler 3 31000 32000 33000 dwrr 20 20 20 10 10
```

Related Commands

class, policy-map

script reload

Reloads scripts from disk and shows a variety of script-related information.

Syntax

script reload [**all** [**debug**]] | **debug** | **diff** [**debug**] | **errors** [**debug**]]

Command Default

None

Parameters

all

Displays information about all scripts.

debug

Displays additional debug information about the scripts.

diff

Displays information about scripts that have changed since the last reload.

errors

Displays information about erroneous scripts.

Modes

Privileged EXEC mode

Examples

To reload scripts from disk:

```
switch# script reload
```

History

Release version	Command history
5.0.1	This command was introduced.

secpolicy activate

Activates the defined switch connection control (SCC) policy and its member set.

Syntax

secpolicy activate [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

Any switch is allowed to join the fabric.

The SCC policy does not exist until it is defined and activated.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The SCC policy is used to restrict which switches can join the fabric by either accepting or rejecting the connection between two switches. Switches are checked against the policy each time an E_Port-to-EX_Port connection is made. The policy is named SCC_POLICY and accepts device members listed as World Wide Names (WWNs).

Although the **active-policy** is listed under the possible completions of **secpolicy** command, the *defined-policy* parameter should be used to create or add policy or members. The **secpolicy activate** command activates the policy.

A defined SCC policy must exist before you can activate the policy. You create the policy with the **secpolicy defined-policy** command.

During configuration replay, the defined and active policies are replayed and the E_Ports are enabled or disabled based on the SCC policy entries in the active policy list.

During **copy file running-config** command execution, only the defined policy in the switch is updated with the config file entries; the active policy entries remain unchanged. In this case, you must use the **secpolicy activate** command to activate the defined policy list.

This command is supported on the Brocade VDX 6740 and Brocade VDX 2740.

Examples

```
switch# secpolicy activate rbridge-id 3
```

Related Commands

secpolicy defined-policy

secpolicy defined-policy

Creates the switch connection control (SCC) policy and adds the SCC defined policy set members (WWNs).

Syntax

secpolicy defined-policy SCC_POLICY [**member-entry** *switch_wwn*]

no secpolicy defined-policy SCC_POLICY [**member-entry** *switch_wwn*]

Command Default

Any switch is allowed to join the fabric.The SCC policy does not exist until it is created.

Parameters

member-entry *switch_wwn*

The switch WWN to be added to the SCC defined policy set.

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

The SCC policy defines which switches can join the fabric by either accepting or rejecting the connection between two switches. Switches are checked against the policy each time an E_Port-to-EX_Port connection is made. The policy is named SCC_POLICY and accepts members listed as WWNs.

When you execute this command, the SCC policy entry is created (if not present) and the WWNs are added to the SCC policy.

This command is not distributed across the cluster. The RBridge ID of the node should be used to configure policy configurations.

Although the **active-policy** is listed under the possible completions of **secpolicy** command, the defined-policy parameter should be used to create or add policy or members. Entering **secpolicy activate** activates the policy.

You can add multiple WWNs separated by a comma.

After you configure the defined SCC_POLICY, run **secpolicy activate** to apply the changes to the active policy set.

This command is supported on the Brocade VDX 6740 and Brocade VDX 2740.

Enter **no secpolicy defined-policy SCC_POLICY member-entry** *switch_wwn* to remove a switch (WWN) from the defined policy member set.

Enter **no secpolicy defined-policy SCC_POLICY** to remove the SCC policy, along with all of the defined policy members.

Examples

To create the defined SCC policy:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# secpolicy defined-policy SCC_POLICY
switch(config-defined-policy-SCC_POLICY)# exit
```

To add a switch WWN to the policy set:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# secpolicy defined-policy SCC_POLICY member-entry 10:00:00:05:1e:
00:69:00
switch(config-member-entry-10:00:00:05:1e:00:69:00)# exit
switch(config-defined-policy-SCC_POLICY)# exit
switch(config-rbridge-id-3)# exit
```

To remove an entry from the policy list of rbridge id 3:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no secpolicy defined-policySCC_POLICY member-entry 10:00:00:05:1e:00:69:01
```

To remove the SCC_POLICY entry of rbridge id 3:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no secpolicy defined-policySCC_POLICY
```

Related Commands

secpolicy activate

security-profile (AMPP)

Activates the security-profile mode for AMPP.

Syntax

security-profile

no security-profile

Modes

Port-profile configuration mode

Usage Guidelines

The security-profile mode for AMPP allows configuration of security attributes of a port-profile.

Enter **no security-profile** to remove the profile.

Examples

To activate the security-profile mode for AMPP:

```
switch(config)# port-profile sample-profile
switch(conf-pp)# security-profile
```

seq (IPv4 extended ACLs)

Inserts filtering rules in IPv4 extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S_port-numbers*] { **any** | *D_IPaddress mask* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S_port-numbers*] { **any** | *D_IPaddress mask* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

no seq *seq-value*

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S_port-numbers*] { **any** | *D_IPaddress mask* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 0 through 4294967290.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

icmp

Internet Control Message Protocol

ip

Any IP protocol

tcp

Transmission Control Protocol

udp
: User Datagram Protocol

any
: Specifies all source addresses.

S_IPaddress
: Specify a source address for which you want to filter the sub-net.

mask
: Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host
: Specifies a source address.

S_IPaddress
: The source address.

(Source Operator)
: The following operators are available:

eq
: The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt
: The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt
: The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq
: The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range
: The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers
: (Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source port numbers.

any
: Specifies all destination addresses.

D_IPaddress
: Specify a destination address for which you want to filter the sub-net.

mask
: Defines a mask, whose effect is to specify a subnet that includes the destination address that you specified. For options to specify the mask, see the Usage Guidelines.

host
: Specifies a destination address.

D_IPaddress
The destination address.

(Destination Operator)
The following operators are available:

eq
The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt
The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt
The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.

D_port_numbers
(Valid only when *ip-protocol* is UDP or TCP) The operator that you specified determines how D_port_numbers are applied.

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63.

count
Enables statistics for the rule.

log
(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination addresses and protocol type. You can also enable counters and logging for specified rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

For an ACL applied to a management interface, **hard-drop** keywords are interpreted as **deny** keywords.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax except for **seq** *seq-value*.

Examples

The following example creates an IPv4 extended ACL and defines rules:

```
switch(config)# ip access-list extended extdACL5
switch(config-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
switch(config-ipacl-ext)# seq 7 deny tcp any any eq 80
switch(config-ipacl-ext)# seq 10 deny udp any any range 10 25
switch(config-ipacl-ext)# seq 15 permit tcp any any
```

Related Commands

ip access-group, ip access-list, show access-list, show running-config access-list

seq (IPv6 extended ACLs)

Inserts filtering rules in IPv6 extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress /prefix_len* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S_port-numbers*] { **any** | *D_IPaddress/prefix_len* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress/prefix_len* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S_port-numbers*] { **any** | *D_IPaddress/prefix_len* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

no seq *seq-value*

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress/ prefix_len* | **host** *S_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *S-port_numbers*] { **any** | *D_IPaddress/prefix_len* | **host** *D_IPaddress* } [{ **eq** | **gt** | **lt** | **neq** | **range** } *D_port-numbers*] [**vlan** *vlanID*] [**dscp** *DSCPvalue*] [**ack** | **fin** | **rst** | **sync** | **urg** | **push**] [**count**] [**log**]

Parameters

seq
: (Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value
: Valid values range from 0 through 4294967290.

permit
: Specifies rules to permit traffic.

deny
: Specifies rules to deny traffic.

hard-drop
: Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol
: Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>
: Protocol number custom value from 0 through 255.

icmp
: Internet Control Message Protocol

ip
: Any IP protocol

tcp
: Transmission Control Protocol

udp
User Datagram Protocol

any
Specifies all source addresses.

S_IPaddress
Specify a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host
Specifies a source address.

S_IPaddress
The specific address. For options to abbreviate the address, see the Usage Guidelines.

(Source Operator)
The following operators are available:

eq
The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt
The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt
The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more port numbers.

any
Specifies all destination addresses.

D_IPaddress
Specify a destination address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host
Specifies a destination address.

D_IPaddress
The destination address. For options to abbreviate the address, see the Usage Guidelines.

(Destination Operator)
The following operators are available:

eq
The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt
The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt
The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.

D_port_numbers
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more destination port numbers.

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63.

count
Enables statistics for the rule.

log
(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination addresses and protocol type. You can also enable counters and logging for specified rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

For an ACL applied to a management interface, **hard-drop** keywords are interpreted as **deny** keywords.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1 are not permitted.)

On the Brocade VDX 8770 under Network OS 5.0.0, filtering of IPv6 traffic by DSCP value is supported for ingress only. On the VDX 4740, VDX 4740T, and VDX 4740T-1G, DSCP-based filtering of IPv6 traffic is also supported for egress.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax except for **seq** *seq-value*.

Examples

The following example shows how to create an IPv6 extended ACL, define a rule for it, and apply the ACL to an interface.

```
switch# configure
switch(config)# ipv6 access-list extended ip_acl_1
switch(conf-ip6acl-ext)# seq 10 deny ipv6 2001:2002:1234:1::/64 2001:1001:1234:1::/64 count
switch(conf-ip6acl-ext)# exit
switch(config)# interface ten 122/5/22
switch(conf-if-te-122/5/22)# ipv6 access-group ip_acl_1 in
```

Related Commands

ipv6 access-group, ipv6 access-list, show access-list, show running-config access-list

seq (IPv4 standard ACLs)

Inserts filtering rules in IPv4 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [**count**] [**log**]

{ **deny** | **permit** | **hard-drop** } { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [**count**] [**log**]

no seq *seq-value*

no { **deny** | **permit** | **hard-drop** } { **any** | *S_IPaddress mask* | **host** *S_IPaddress* } [**count**] [**log**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 0 through 4294967290.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source addresses.

S_IPaddress

Specifies a source address for which you want to filter the subnet.

mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.

S_IPaddress

The source address.

count

Enables statistics for the rule.

log

(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters and logging for specified rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

For an ACL applied to a management interface, **hard-drop** keywords are interpreted as **deny** keywords.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Examples

The following example shows how to create a IPv4 standard ACL, define rules for it, and apply the ACL to an interface:

```
switch# configure
switch(config)# ip access-list standard stdACL3
switch(config-ipacl-std)# seq 5 permit host 10.20.33.4
switch(config-ipacl-std)# seq 15 deny any
switch(config-ipacl-std)# exit
switch(config)# interface ten 122/5/22
switch(conf-if-te-122/5/22)# ipv4 access-group stdACL3 in
```

Related Commands

ip access-group, ip access-list, show access-list, show running-config access-list

seq (IPv6 standard ACLs)

Inserts filtering rules in IPv6 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *S_IPaddress* } [**count**] [**log**]

{ **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**]

no seq *seq-value*

no { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 0 through 4294967290.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source addresses.

S_IPaddress

Specify a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len

Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host

Specifies a source address.

SIP_address

The source address. For options to abbreviate the address, see the Usage Guidelines.

count

Enables statistics for the rule.

log

(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters and logging for specified rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

For an ACL applied to a management interface, **hard-drop** keywords are interpreted as **deny** keywords.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1 are not permitted.)

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Examples

The following example shows how to create an IPv6 standard ACL and define rules for it:

```
switch(config)# ipv6 access-list standard ipv6-std-acl
switch(conf-ip6acl-std)# seq 10 permit host 0:1::1
switch(conf-ip6acl-std)# seq 20 deny 0:2::/64
switch(conf-ip6acl-std)# seq 30 hard-drop any count
```

Related Commands

ipv6 access-group, ipv6 access-list, show access-list, show running-config access-list

seq (MAC extended ACLs)

Inserts filtering rules in a Layer 2 (MAC) extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*EtherType* | **arp** | **fcoe** | **ipv4**] [**count**] [**log**]

{ **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*EtherType* | **arp** | **fcoe** | **ipv4**] [**vlan** *vlanID*] [**count**] [**log**]

no seq *seq-value*

no seq { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*EtherType* | **arp** | **fcoe** | **ipv4**][**count**] [**log**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 0 through 4294967290.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source MAC addresses.

SMAC_address

Specifies a source MAC address and a comparison mask.

mask

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host

Specifies a source MAC address.

SMAC_address

Use the format HHHH.HHHH.HHHH.

any
Specifies all destination MAC addresses.

DMAC_address
Specify a destination MAC address and a comparison mask.

mask
Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host
Specifies a destination MAC address.

DMAC_address
Use the format HHHH.HHHH.HHHH.

EtherType
Specifies the protocol number for which to set the permit or deny conditions. Valid values range from 1536 through 65535.

arp
Specifies to permit or deny the Address Resolution Protocol (0x0806).

fcoe
Specifies to permit or deny the Fibre Channel over Ethernet Protocol (0x8906).

ipv4
Specifies to permit or deny the IPv4 protocol (0x0800).

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

count
Enables statistics for the rule.

log
(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination MAC addresses and protocol type. You can also enable counters and logging for specific rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value* .

Examples

The following example creates a rule in a MAC extended ACL to deny IPv4 traffic from the source MAC address 0022.3333.4444 to the destination MAC address 0022.3333.5555 and to enable the counting of packets:

```
switch(conf-macl-ext)# seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count
```

The following example deletes a rule from a MAC extended ACL:

```
switch(conf-macl-ext)# no seq 100
```

Related Commands

mac access-group, mac access-list extended, show access-list, show running-config access-list

seq (MAC standard ACLs)

Inserts filtering rules in Layer 2 (MAC) standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**]

{ **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**]

no seq *seq-value*

no seq { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 0 through 4294967290.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames and data frames such as echo request (ping). However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source MAC addresses.

SMAC_address

Specifies a source MAC address and a comparison mask.

mask

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host

Specifies a source MAC address.

SMAC_address

Use the format HHHH.HHHH.HHHH.

count

Enables statistics for the rule.

log

(Available for **permit** or **deny** only) Enables logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source MAC address. You can also enable counters and logging for specific rules.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The hard-drop option can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For more information, refer to the "Configuring QoS" > "Flow-based QoS" section of the *Network OS Layer 2 Switching Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not implemented.
- The **hard-drop** keyword is equivalent to the **deny** keyword.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax, without **seq** *seq-value*.

Examples

The following command creates statistic-enabled rules in a MAC standard ACL:

```
switch(conf-macl-std)# seq 100 deny host 0022.3333.4444 count
switch(conf-macl-std)# seq 110 permit host 0011.3333.5555 count
```

The following command deletes a rule in a MAC standard ACL:

```
switch(conf-macl-std)# no seq 100
```

Related Commands

mac access-group, mac access-list standard, resequence access-list, show access-list, show running-config access-list

service password-encryption

Enables or disables password encryption.

Syntax

service password-encryption

no service password-encryption

Command Default

Default value is service password-encryption.

Modes

Global configuration mode

Usage Guidelines

Enter **no service password-encryption** to disable password encryption.

Examples

To enable password encryption:

```
switch(config)# service password-encryption
```

To disable password encryption:

```
switch(config)# no service password-encryption
```

Related Commands

show running-config password-attributes

service-policy

Binds a policy-map to an interface.

Syntax

service-policy in | **out** *policy-mapname*

no service-policy in | **out**

Command Default

No service policy is created.

Parameters

in
Binds policy-map to inbound traffic.

out
Binds policy-map to outbound traffic.

policy-mapname
Name of the policy-map.

Modes

Interface subtype configuration mode

Usage Guidelines

This command applies a policy-map containing a class-map with specific Policer parameters and match critters to a switch interface. The policy-map must be configured before you can apply it (refer to the description of the **policy-map** command).

The **no** form of this command emoves the service policy.

NOTE
This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To create a service-policy for outbound traffic on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8

switch(conf-if-te-237/1/8)# service-policy out policymap1
```

To remove a service-policy for outbound traffic from a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8
switch(conf-if-te-237/1/8)# no service-policy out
```

To remove a service-policy for inbound traffic on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 237/1/8
switch(conf-if-te-237/1/8)# no service-policy in
```

Related Commands

interface, class, qos cos, policy-map, show policymap

set as-path

Sets a prepended string or a tag for a BGP AS-path attribute in a route-map instance.

Syntax

set as-path [**prepend** *string* | **tag**]

no set as-path [**prepend** *string* | **tag**]

Parameters

prepend

Prepends the string to the AS-path.

string

AS numbers. Range is from 1 through 4294967295.

tag

Sets a route tag.

Modes

Route-map configuration mode

Related Commands

route-map

set as-path prepend

Prepends an AS4 number to an AS path, makes the AS number a tag attribute for a route map, and provides a variety of route-management options.

Syntax

set as-path prepend *as-num* **,** *as-num* **, . . .** *as-num* [**automatic-tag**] | [**comm-list** *acl* **delete**] | [**community** *num* **:** *num* | *num* | **additive** | **internet** | **local-as** | **no-advertise** | **no-export**] | [**dampening** [*half-life* | *reuse* | *suppress* | *max-suppress-time*]] [**ip next hop** *ip-addr*] [**ip next-hop peer-address**] | [**local-preference** *num*] | [**metric** [**add** | **assign** | **none** | **sub**]] | [**metric-type** [**type-1** | **type-2**]] | **external** [**metric-type internal**] | [**origin igp** | **incomplete**] | [**tag**] | [**weight** *num*]

no set as-path prepend *as-num* **,** *as-num* **, . . .** *as-num*

Parameters

automatic-tag
Calculates and sets an automatic tag for the route.

comm-list *acl* **delete**
Deletes a community from the community attributes field for a BGP4 route.

community
Sets the community attribute for the route to the number or well-known type specified. Possible values are *num* : *num* , Internet, no-export, local-as, no-advertise.

num:*num*
Specific community member.

additive
Adds a community to the already existing communities.

internet
The Internet community.

local-as
Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.

no-advertise
Routes with this community cannot be advertised to any other BGP4 devices at all.

no-export
Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGP neighbors.

dampening
Sets dampening parameters for the route.

half-life
Number of minutes after which the route penalty becomes half its value.

reuse
Specifies how low a route penalty must become before the route becomes eligible for use again after being suppressed.

suppress
Specifies how high a route penalty can become before the device suppresses the route.

max-suppress-time
Specifies the maximum number of minutes that a route can be suppressed regardless of how unstable it is.

ip next hop
Sets the next-hop IP address for a route that matches the match statement in the route map.

ip-addr
IPv4 address in dotted-decimal notation.

ip next-hop peer-address
Sets the BGP4 next hop for a route to the neighbor address.

local-preference
Sets the local preference for the route.

num
Range is from 0 through 4294967295.

metric
Sets the MED (metric) value for the route. Range is from 0 through 4294967295. The default MED value is 0.

add
Adds to the current metric value.

assign
Replaces the current metric value with a new value.

none
Removes the MED attribute (metric) from the BGP4 route.

sub
Subtracts from the current metric value.

metric-type
Changes the metric type of the route redistributed into OSPF.

type-1
Type 1 route.

type-2
Type 2 route.

external
External Type 1 or Type 2 route.

metric-type internal
Sets route MED attribute to same value as the IGP metric of the BGP4 next-hop route, for advertising a BGP4 route to an EBGP neighbor.

next-hop
Sets IPv4 address of the next hop.

ip-addr
IPv4 address in dotted-decimal notation.

origin
Sets the route's origin.

igp
Sets origin to IGP.

incomplete
Sets origin to INCOMPLETE.

tag
Keyword that makes the ASN an AS-path tag attribute. (Applies only to routes redistributed into OSPF.)

weight
Sets the weight for the route.

num
Range is from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the configuration.

Examples

To prepend an AS4 number:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# route-map myroutes
switch(config-route-map myroutes)# set as-path prepend 7701000
```

Related Commands

route-map

set automatic-tag

Sets the route-map tag value.

Syntax

set automatic-tag *value*

Parameters

value

The value for the computed tag.

Modes

Route-map configuration mode

Usage Guidelines

This command sets an automatically computed tag value in a route-map instance.

Related Commands

route-map

set comm-list

Sets a BGP community list for deletion in a route-map instance.

Syntax

set comm-list *name*

no set comm-list *name*

Parameters

name

BGP community list name. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** version of this command to disable this feature.

Related Commands

route-map

set community

Sets a BGP community attribute in a route-map instance.

Syntax

set community [*community-number* | *local-as* | *no-advertise* | *no-export* | *none*]

no set community *community-number*

Parameters

community-number
BGP community number, in two format options:(1) Range is from 1 through 4294967295.(2) Format is AA:NN, where AA is the AS number, and NN is a locally significant number.

local-as
Do not send outside local AS (well-known community).

no-advertise
Do not advertise to any peer (well-known community).

no-export
Do not export to next AS (well-known community).

none
Sets no community attribute.

Modes

Route-map configuration mode

Related Commands

route-map

set cos traffic-class

Specifies the User-Priority field value in VLAN header and traffic-class queuing value when a packet matches a flow.

Syntax

set cos { 0..7 } **traffic-class** { 0..7 }

no set cos { 0..7 } **traffic-class** { 0..7 }

Parameters

0..7

Modifies the Class of Service (CoS) value in the VLAN header of classified traffic, or assigns a queue to the classified traffic. The range of valid values is from 0 through 7.

Modes

Route-map configuration mode

Examples

```
switch(config)# policy-map p1
switch(config-policymap)# class c1
switch(config-policyclass)# set cos 4 traffic-class 3
```

Related Commands

class, policy-map

set dampening

Sets a BGP route-flap dampening penalty in a route-map instance.

Syntax

set dampening *number*

no set dampening *number*

Command Default

The default is 15.

Parameters

number

Half-life in minutes for the penalty. Range is from 1 through 45.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of this commands removes the penalty.

Related Commands

route-map

set distance

Sets the administrative distance for matching OSPF routes in route-map instance.

Syntax

set distance *value*

no set distance

Parameters

value

Administrative distance for the route. Range is from 1 through 254.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of this command removes the configuration.

Related Commands

ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set ip next-hop, set metric, set tag

set dscp

Specifies the DSCP field value in IP header when a packet matches a flow.

Syntax

set dscp { **0..63** }

no set dscp { **0..63** }

Parameters

0..63

The DSCP value in the IP header of the classified traffic. The range of valid values is from 0 through 63.

Modes

Route-map configuration mode

Examples

```
switch(config)#policy-map p1
switch(config-policymap)#class c1
switch(config-policyclass)#set dscp 56
```

Related Commands

class, policy-map

set extcommunity

Sets an extended BGP community attribute in a route-map instance.

Syntax

set extcommunity { **rt** *extcommunity value* | **soo** *extcommunity value* }

no set extcommunity

Command Default

No extended BGP community attribute is set in a route-map instance.

Parameters

rt
Specifies the route target (RT) extended community attribute.

soo
Specifies the site of origin (SOO) extended community attribute.

extcommunity value
Specifies the value. The value can be one of the following:

ASN:nn—autonomous-system-number:network-number
Autonomous system (AS) number and network number.

IPAddress:nn—ip-address:network-number
IP address and network number.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no set extcommunity** to delete an extended community set statement from the configuration file.

Examples

To set the route target to extended community attribute 1:1 for routes that are permitted by the route map:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity rt 1:1
```

To set the site of origin to extended community attribute 2:2 for routes that are permitted by the route map:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ip community-list extended 1 permit 123:2
device(config-rbridge-id-122)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity soo 2:2
```

History

Release version	Command history
5.0.0	This command was introduced.

set ip interface null0

Drops traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process..

Syntax

set ip interface null0

no set ip interface null0

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of this command deletes the matching filter from the ACL.

Related Commands

ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set metric, set tag

set ip next-hop

Sets the IPv4 address of the next hop in a route-map instance.

Syntax

set ip [**global** | **vrf** *vrf-name*] **next-hop** *A.B.C.D*

no set ip next-hop *A.B.C.D*

Parameters

A.B.C.D
IPv4 address of the next hop.

global
Specifies that the next specified hop address is to be resolved from the global routing table.

vrf *vrf-name*
Specifies from which VRF routing table the specified next hop address will be resolved.

next hop *A.B.C.D*
Sets the next hop to which to route the packet. The next hop must be adjacent.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to delete the matching filter from the ACL.

Related Commands

ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set metric, set tag

set ipv6 next-hop

Sets the IPv6 address of the next hop in a route-map instance.

Syntax

set ipv6 [**global** | **vrf** *vrf-name*] **next-hop** *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

no set ipv6 next-hop *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

Parameters

AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH
IPv6 address of the next hop.

global
Specifies that the next specified hop address is to be resolved from the global routing table.

vrf *vrf-name*
Specifies from which VRF routing table the specified next hop address will be resolved.

next hop *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*
Sets the next hop to which to route the packet. The next hop must be adjacent.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to delete the matching filter from the ACL.

set local-preference

Sets a BGP local-preference path attribute in a route-map instance.

Syntax

set local-preference *number*

no set local-preference

Parameters

number

Range is from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the attribute.

Related Commands

route-map

set metric

Configures the route metric set clause in a route-map instance.

Syntax

set metric [**add** | **assign** | **sub**] *value*

no set metric [**add** | **assign** | **sub**] *value*

Parameters

add
Adds the value to the current route metric.

assign
Replaces the current route metric with this value.

sub
Subtracts the value from the current route metric.

none
Removes the current route metric.

value
Range is from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the configuration.

Related Commands

ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set tag

set metric-type

Sets a variety of metric types for destination routing in a route-map instance.

Syntax

set metric-type [*external* | *internal* | *type-1* | *type-2*]

no set metric-type [*external* | *internal* | *type-1* | *type-2*]

Parameters

external
IS-IS external metric

internal
IGP internal metric to BGP MED

type-1
OSPF external type-1 metric

type-2
OSPF external type-2 metric

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the configuration.

Related Commands

route-map

set origin

Sets a BGP origin code in a route-map instance.

Syntax

set origin [*igp* | *incomplete*]

no set origin [*igp* | *incomplete*]

Parameters

igp
Local IGP

incomplete
Unknown heritage

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the configuration.

Related Commands

route-map

set-priority

Configures the priority map of a class-map.

Syntax

set-priority *priority-map-name*

no set-priority *priority-map-name*

Parameters

priority-map-name

The priority-map name that you are including in the policy-map. Refer to the description of the **police-priority-map** command.

Modes

Class-map configuration mode

Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** form of this command to remove the parameter from the class-map.

Examples

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch (config-policymap-class)# set-priority default
```

Related Commands

cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy

set route-type

Sets a route type in a route-map instance.

Syntax

set route-type [*internal* | *type-1* | *type-2*]

no set route-type

Parameters

internal
Internal route type

type-1
OSPF external route type 1

type-2
OSPF external route type 2

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of this command removes the configuration.

set tag

Sets the route tag value in a route-map instance.

Syntax

set tag *value*

no set tag *value*

Parameters

value

The tag clause value for the route-map. Range is from 0 through 4294967295.

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of this command disables this feature.

Related Commands

ip prefix-list, match interface, match ip address, match ip next-hop, match metric, match route-type, match tag, route-map, set distance, set ip next-hop, set metric

set weight

Sets a BGP weight for the routing table in a route-map instance.

Syntax

set weight *number*

no set weight *number*

Parameters

number

Weight value. Range is from 0 through 65535.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of this command disables this feature

Related Commands

route-map

sflow collector

Identifies the sFlow collectors to which sFlow datagrams are forwarded.

Syntax

sflow collector [*IPv4address* | *IPv6address*]

no sflow collector [*IPv4address* | *IPv6address*]

Parameters

IPv4address
Specifies an IPv4 address in dotted-decimal format for the collector.

IPv6address
Specifies an IPv6 address for the collector.

Modes

Global configuration mode

Usage Guidelines

You can only specify up to five sFlow collectors.

The **no** form of this command resets the specified collector address to a null value.

Examples

To identify the sFlow collectors for anIPv4 address to which sFlow datagrams are forwarded:

```
switch(config)# sflow collector 192.10.138.176
```

To identify the sFlow collectors for an IPv6 address and port to which sFlow datagrams are forwarded:

```
switch(config)# sflow collector 3ff3:1900:4545:3:200:f8ff:fe21:67cf:6343
```

sflow enable (global version)

Enables sFlow globally.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is disabled on the system.

Modes

Global configuration mode

Usage Guidelines

This command is supported on physical ports only.

On a Brocade VDX 8770, SPAN and sFlow can be enabled at the same time.

The **no** form of this command disable sFlow globally.

Examples

To enable sFlow globally:

```
switch(config)# sflow enable
```

Related Commands

sflow enable (interface version)

sflow enable (interface version)

Enables sFlow on an interface. sFlow is used for monitoring network activity.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is disabled on all interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is supported on physical ports only.

On a Brocade VDX 8770 switch, SPAN and sFlow can be enabled at the same time.

The **no** form of this command disable sFlow on an interface.

Examples

To enable sFlow on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow enable
```

Related Commands

interface, sflow enable (global version), sflow polling-interval (interface version), sflow sample-rate (interface version)

sflow polling-interval (global version)

Configures the polling interval globally.

Syntax

sflow polling-interval *interval_value*

no sflow polling-interval

Parameters

interval_value

Specifies a value in seconds to set the polling interval. Valid values range from 1 through 65535 seconds.

Command Default

The default is 20.

Modes

Global configuration mode

Usage Guidelines

The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

The **no** form of this command restores the default value.

Examples

To set the polling interval to 135 seconds:

```
switch(config)# sflow polling-interval 135
```

Related Commands

sflow polling-interval (interface version)

sflow polling-interval (interface version)

Configures the polling interval at the interface level.

Syntax

sflow polling-interval *interval_value*

no sflow polling-interval

Command Default

The defaut is 20.

Parameters

interval_value

Specifies a value in seconds to set the polling interval. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

The **no** form of this command restores the default value.

Examples

To set the polling interval to 135 seconds on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow polling-interval 135
```

Related Commands

interface, sflow polling-interval (global version), sflow enable (interface version), sflow sample-rate (interface version)

sflow sample-rate (global version)

Sets the number of packets that are skipped before the next sample is taken.

Syntax

sflow sample-rate *samplerate*

no sflow sample-rate

Command Default

The default is 32768.

Parameters

samplerate

Specifies the sampling rate value in packets. Valid values range from 2 through 16777215 packets.

Modes

Global configuration mode

Usage Guidelines

Sample-rate is the average number of packets skipped before the sample is taken.

The **no** form of this command restores the default sampling rate.

Examples

To change the sampling rate to 4096:

```
switch(config)# sflow sample-rate 4096
```

Related Commands

sflow polling-interval (interface version)

sflow sample-rate (interface version)

Sets the default sampling rate for an interface.

Syntax

sflow sample-rate *samplerate*

no sflow sample-rate

Command Default

The default is 32768.

Parameters

samplerate

Specifies the sampling rate. Valid values range from 2 through 16777215 packets.

Modes

Interface subtype configuration mode

Usage Guidelines

The default sampling rate determines how many packets are skipped before the next sample is taken for that interface. The default sampling rate of an interface is set to the same value as the current global default sampling rate.

This command changes the sampling rate for an interface.

The **no** form of this command restores the default setting.

Examples

To change the sampling rate to 4096 packets on a specific 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(conf-if-fo-1/3/1)# sflow sample-rate 4096
```

Related Commands

interface, sflow sample-rate (global version), sflow enable (interface version), sflow polling-interval (interface version)

sflow-profile

Establishes an sFlow profile name and sets a sampling rate.

Syntax

sflow-profile { *sflow_profile_name* } { **sample-rate** *sampling_rate* }

no sflow-profile { *sflow_profile_name* }

Command Default

This command is disabled.

Parameters

sflow_profile_name
Name of an sFlow profile for sampling rates. The maximum number of characters is 64.

sample-rate
Selects a sampling rate.

sampling_rate
Specifies a sampling rate. Range is from 2 through 8388608 packets, in powers of 2 only. The default is 32768 packets.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables the sFlow profile.

Examples

To establish an sFlow profile and set a sampling rate of 4096:

```
switch(config)# sflow mysflowprofile sample-rate 4096
```

sflow profile-map

Attaches an sFlow profile map to a class map in flow-based QoS. This configures the sampling rate and other sFlow attributes.

Syntax

sflow profile-map *map_name*

Command Default

The sFlow profile map must be created.

Parameters

map_name

The sFlow profile map to attach to the class map in flow-based QoS. The maximum number of characters is 64.

Modes

Policy-map configuration mode

Usage Guidelines

Specifying a non-existent map name causes an error.

This action is allowed only in the ingress direction.

It can be configured both in user-defined class maps and in the class map "default". If configured in the class map "default", port-based sFlow is enabled.

Examples

Typical command execution.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)#class cmap1
switch(config-policyclass)#sflow profile-map mysflowprofile
```

History

Release version	Command history
5.0.0	This command was introduced.

sflow (VXLAN)

Enables sFlow monitoring of the tunnel endpoints for a VXLAN overlay gateway site.

Syntax

sflow *profile_name* **remote-endpoint** { *IPv4_address* | **any** } **vlan** { **add** | **remove** } *vlan_id* [**vrf** *name*]

no sflow *profile_name*

Parameters

profile_name
Name of a configured sFlow profile.

remote-endpoint
Specifies an IPv4 address or all IPv4 addresses associated with the remote tunnel endpoint for the site.

IPv4_address
IPv4 address for the tunnel endpoint.

any
Specifies all IPv4 addresses for the tunnel endpoint.

vlan
Specifies a VLAN ID or range of VLAN IDs to be added or removed from the tunnel.

add
Specifies a VLAN ID or range of VLAN IDs to be added to the tunnel.

remove
Specifies a VLAN ID or range of VLAN IDs to be removed from the tunnel.

vlan_id
A VLAN ID or range of VLAN IDs. See the Usage Guidelines.

vrf
Specifies a VRF instance.

name
Name of the VRF instance.

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

An sFlow profile must be configured, by means of the **sflow-profile** command.

Use the **no sflow** *profile_name* command to remove the configuration from the overlay gateway.

Examples

To enable sFlow monitoring for all endpoints for specified VLAN IDs:

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# sflow my_sflow_profile remote-endpoint any vlan add 10,20-30
```

sfp breakout

Allows a single physical 40G or 100G port to be utilized as multiple 10G ports. For example, a 40G port can be configured to operate as four individual 10G external ports

Syntax

sfp breakout [**speed***speed_value*]

no sfp breakout

Parameters

speed *speed*

Specifies the size of the breakout ports. The valid values are 10 and 40.

Command Default

Breakout mode is set to disabled.

Modes

Connector configuration mode

Usage Guidelines

If you do not specify a speed, the system automatically configures the port into multiple 10G ports.

The port must not be a member of a port channel.

NOTE

For the 27x40 GbE line card on a Brocade VDX 8770, a port group must be in performance mode before you can configure one of its ports to breakout mode.

Use the **no sfp breakout** to disable breakout mode and restore the interface.

Examples

To enable SFP breakout on a connector:

```
switch# configure terminal
switch(config)# hardware
switch(config-hardware)# connector 2/0/1
switch(config-connector-2/0/1)# sfp breakout 10
switch(config-connector-2/0/1)# do copy running-config startup-config
```

To disable SFP breakout on a connector:

```
switch(config-connector-2/0/1)# no sfp breakout
```

Related Commands

power-off linecard, power-on linecard

shape

Specifies the shaping rate for a port to smooth out the traffic egressing an interface

Syntax

shape *speed*

Parameters

speed

The speed for the shape rate in Kbps. The range of valid values is from 28000 to the top speed on the interface.

Modes

Policymap configuration mode

Usage Guidelines

This command is allowed only for the Egress direction.

This command can only be configured in for the **class class-default** command.

This command is mutually exclusive of the **scheduler** and **police** commands.

The minimum speed for a Brocade VDX 6740 is 200,000 Kbps.

Examples

Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# shape 30000
```

Related Commands

class, policy-map

short-path-forwarding

Enables short-path forwarding on a VRRP router.

Syntax

short-path-forwarding [**revert-priority** *number*]

no short-path-forwarding

Command Default

Disabled

Parameters

revert-priority *number*

Allows additional control over short-path-forwarding on a backup router. If you configure this option, the revert-priority number acts as a threshold for the current priority of the session, and only if the current priority is higher than the revert-priority will the backup router be able to route frames. The range of revert-priority is 1 to 254.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Short-path forwarding means that a backup physical router in a virtual router attempts to bypass the VRRP-E master router and directly forward packets through interfaces on the backup router.

This command can be used for VRRP-E, but not for VRRP. You can perform this configuration on a virtual Ethernet (VE) interface only.

Enter **no short-path-forwarding** to remove this configuration.

Examples

To enable short-path-forwarding on a VRRP-E group:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 25
switch(config-ve-25)# vrrp-extended-group 100
switch(config-vrrp-extended-group-100)# short-path-forwarding
```

Show commands

show access-list

For a given network protocol and inbound/outbound direction, displays ACL status information. You can show information for a specified ACL or only for that ACL on a specified interface. You can also display information for all ACLs bound to a specified switch interface, VLAN, VE, or VXLAN overlay-gateway.

Syntax

For a specified network protocol (MAC, IPv4, or IPv6), the following version displays general information about all ACLs applied to the switch:
show access-list { **ip** | **ipv6** | **mac** }

The following version displays information for either the inbound or the outbound direction of a specified ACL:
show access-list { **ip** | **ipv6** | **mac**} *name* { **in** | **out** }

For either the inbound or the outbound direction on a specified N-gigabite physical Ethernet, port-channel, VLAN, or management interface, the following version displays information for all ACLs bound to that interface:
show access-list interface { *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* | **management** *rbridge_id/port* } { **in** | **out** }

For either the inbound or the outbound direction on a specified virtual Ethernet (VE) interface, the following version displays information for all ACLs bound to that interface. You can also include ACLs on nodes connected by RBridges:
show access-list interface ve *vlan_id* { **in** | **out** } [**rbridge-id** { *rbridge_id* | **all** }]

For the inbound direction on a specified VXLAN overlay-gateway, the following version displays information for all ACLs bound to that overlay gateway:
show access-list overlay-gateway *overlay_gateway_name* **in**

For either the inbound or the outbound direction, on a specified N-gigabite physical Ethernet, port-channel, or VLAN interface, the following version displays the rules in a specified MAC ACL bound to that interface:
show access-list mac *name* **interface** { *<N>*-**gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

For either the inbound or the outbound direction, on a specified N-gigabite physical Ethernet, port-channel, VLAN, or management interface, the following version displays the rules in a specified Layer 3 ACL bound to that interface:
show access-list *name* **interface** { *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* | **management** *rbridge_id/port* } { **in** | **out** }

For either the inbound or the outbound direction, on a specified virtual Ethernet (VE) interface, the following version displays the rules in a specified Layer 3 ACL bound to that interface. You can also include ACLs on nodes connected by RBridges:
show access-list *name* **interface ve** *vlan_id* **in** | **out** } [**rbridge-id** { *rbridge_id* | **all** }]

Parameters

ip | **ipv6** | **mac**
: Specifies the network protocol.

name
: Specifies the ACL name.

interface
Filters by interface.

<*N*>**gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace **<*N*>gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge_id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

management *rbridge_id/port*
Specifies a management interface.

port-channel *index*
Specifies a port-channel interface.

vlan *vlan_id*
Specifies a VLAN interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

rbridge-id
(for a VE interface) To display ACLs beyond the local node, include this keyword and the relevant of the following:

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

overlay-gateway *overlay_gateway_name*
Specifies a VXLAN overlay-gateway.

in | **out**
Specifies the ACL binding direction (incoming or outgoing).

Modes

Privileged EXEC mode

Usage Guidelines

On the Brocade VDX family of hardware, VLANs are treated as interfaces from a configuration point of view. By default all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). For details of valid VLAN IDs, refer to the **vlan classifier group** command.

Command Output

The **show access-list** command displays the following information:

Output field	Description
Active	The rule is active and implements the configured action.
Partial	The rule is partially programmed, with the configured action implemented in some cases. This is typically seen for logical interfaces like VLAN, which span multiple hardware resources.
In progress	The rule is currently being programmed into the hardware.
Inactive	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays the names of IPv4 ACLs applied to the switch, interfaces to which they are applied, and incoming/outgoing direction:

```
sw0# show access-list ip
Interface Ve 171
   Inbound access-list is not set
   Outbound access-list is IPV4_ACL_000 (From User)
```

The following example displays all interfaces on which an IPv4 ACL is applied in the outgoing direction:

```
sw0# show access-list ip IPV4_ACL_000 out
ip access-list IPV4_ACL_000 on Ve 171 at Egress (From User)
    seq 0 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
```

The following example displays all interfaces on which an IPv6 ACL is applied in the incoming direction:

```
switch# show access-list ipv6 distList in
ipv6 access-list distList on TenGigabitEthernet 122/1/2 at Ingress (From User)
    seq 10 deny 2001:125:132:35::/64 (Active)
    seq 20 deny 2001:54:131::/64 (Active)
    seq 30 deny 2001:5409:2004::/64 (Active)
    seq 40 permit any (Active)
```

The following example displays all ACLs applied on a specified interface in the outgoing direction:

```
switch# show access-list interface tengigabitethernet 1/4/1 in
ipv6 access-list ipv6-std-acl on TenGigabitEthernet 1/4/1 at Ingress (From User)
    seq 10 permit host 0:1::1 (Active)
    seq 20 deny 0:2::/64 (Active)
    seq 30 hard-drop any count (Active)
```

The following example displays details of ACLs applied in the outgoing direction to VE 121, RBridge 2.

```
sw0# show access-list interface ve 171 out rbridge-id 2
ip access-list IPV4_ACL_000 on Ve 171 at Egress (From User)
    seq 0 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
```

The following example displays information for ACLs applied to a VXLAN overlay-gateway named gw121:

```
switch# show access-list overlay-gateway gw121 in
mac access-list stdmacaclin on overlay-gateway gw121 at Ingress (From User)
ip access-list stdipaclin on overlay-gateway gw121 at Ingress (From User)
  seq 0 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
ipv6 access-list stdipv6aclin on overlay-gateway gw121 at Ingress (From User)
  seq 10 permit host 0:1::1 (Active)
  seq 20 deny 0:2::/64 (Active)
  seq 30 hard-drop any count (Active)
```

Related Commands

access-group, access-list, show running-config access-list, show statistics access-list

show access-list-log buffer

Displays the contents of the log buffer for all ACLs.

Syntax

show access-list-log buffer

Modes

Privileged EXEC mode

Examples

Sample terminal output:

```
switch# show access-list-log buffer
Frames Logged on interface 1/2/1 :
--------------------------------
Frame Received Time : Fri Dec 9 3:8:48 2011
Ethernet,       Src : (00:34:56:78:0a:ab), Dst: (00:12:ab:54:67:da)
  Ethtype           : 0x8100
  Vlan tag type     : 0x800
  VlanID            : 0x1
Internet proto, Src : 192.85.1.2, Dst: 192.0.0.1
  Interface         :
  Type of service   : 0
  Length            : 110
  Identification    : 0
  Fragmentation     : 00 00
  TTL               : 255
  protocol          : 253
  Checksum          : 39 3a
  Payload type      :
packet(s) repeated  : 30
-------------------------------------------------------------------------
```

Related Commands

access-group, access-list, show access-list, show access-list-log buffer config

show access-list-log buffer config

Displays the configuration of the ACL buffer.

Syntax

show access-list-log buffer config

Modes

Privileged EXEC mode

Examples

Sample terminal output:

```
switch# show access-list-log buffer config
ACL Logging Enabled.
ACL logging Buffer configuration: Buffer type is circular and Buffer size is 1600.
```

Related Commands

access-group, access-list, show access-list, show access-list-log buffer

show ag

Displays the current Access Gateway configuration on a switch.

Syntax

show ag [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID for the switch.

Modes

Privileged EXEC mode

Usage Guidelines

The command displays current, active configuration information for Access Gateway, such as the switch identification, number and type of ports, enabled policies, port grouping, and attached fabric details

Consider these guidelines when automatic login balancing (lb) mode is enabled or disabled for a port group.

- When lb mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the configured VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, the **show ag** and **show ag mapcommands** display the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples

Following is an example of the Access Gateway configuration on RBridge 5:

```
sw0# show ag
Rbridge-ID 5:
------------------------------------------------------------
Name : sw0
NodeName : 10:00:00:05:33:f4:78:04
Number of Ports : 32
IP Address(es) : 10.37.209.80
Firmware Version : v4.1.0pgoel_pit02_nos4_1_10_10
Number of N_Ports(Fi) : 2
Number of VF_Ports : 0
Policies Enabled : pg
Persistent ALPA : Disabled
Port Group information :
PG_ID PG_Name PG_Mode PG_Members
-----------------------------------------------------
0 pg0 lb 5/0/1, 5/0/2, 5/0/3, 5/0/4,
5/0/5, 5/0/6, 5/0/7, 5/0/8
------------------------------------------------------------
Fabric Information :
Attached Fabric Name N_Ports(Fi)
------------------------------------------------------------
10:00:00:05:33:72:f5:5a 5/0/1, 5/0/2
N_Port(Fi) information :
Port PortID Attached PWWN IP_Addr VF_Ports
------------------------------------------------------------------------------
Fi 5/0/1 0x020200 20:02:00:05:33:72:f5:5a 10.37.209.86 None
798 Network OS Command Reference
53-1003226-01
5 show ag
Fi 5/0/2 0x020300 20:03:00:05:33:72:f5:5a 10.37.209.86 None
------------------------------------------------------------------------------
VF_Port information :
VF_Port Eth_Port PortID Attached PWWN N_Port(Fi)
------------------------------------------------------------------------------
None
------------------------------------------------------------------------------
```

Related Commands

ag, ag enable, show ag map, show running-config ag

show ag map

Displays the current VF_Port mapping to N_Ports in Access Gateway mode on a specific switch or on all switches in the VCS cluster.

Syntax

show ag map *nport* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

nport
N_Port number supported by the switch model in /rbridge-id/port group/N Port format.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

To display VF_Ports currently mapped to N_Ports on a specific switch, enter **show ag map rbridge-id** *rbridge-id.*

To display VF_Ports currently mapped to a specific N_Port on a specific switch, enter **show ag map** *nport* **rbridge-id** *rbridge-id*. In Network OS commands, N_Ports are designated by the format rbridge-id/port group/N_Port. Therefore, N_Port 5/0/1 designates that N_Port 1 resides in port group 0 on RBridge 5. The **show ag map command** for this N_Port would be the following:

```
show ag map 5/0/1 rbridge-id 5
```

To display VF_Ports currently mapped to a specific N_Port on all switches in the VCS cluster, enter **show ag map** *nport* **rbridge-id all**.

Consider these guidelines when Automatic Login Balancing (LB) mode is enabled or disabled for a port group.

- When Login Balancing (LB) mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the configured VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, the **show ag** and **show ag mapcommands** display the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples

Displaying port mapping information for a switch.

```
sw0# show ag map rbridge 5
Rbridge-ID 5:
--------------------------------------------------
N_Port(Fi) PG_ID PG_Name Current_VF_Ports
--------------------------------------------------
5/0/1 0 pg0 None
5/0/2 0 pg0 None
5/0/3 0 pg0 None
5/0/4 0 pg0 None
5/0/5 0 pg0 None
800 Network OS Command Reference
53-1003226-01
5 show ag map
5/0/6 0 pg0 None
5/0/7 0 pg0 None
5/0/8 0 pg0 None
--------------------------------------------------
```

Related Commands

ag, ag enable, map fport interface fcoe, show ag, show ag nport-utilization, show ag pg

show ag nport-utilization

Displays Access Gateway N_Port utilization information. You can display this information either for a specific RBridge or for all.

Syntax

show ag nport-utilization [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

You can display N_Port utilization information either for a specific RBridge or for all.

rbridge-id

Specify an RBridge ID.

all

Display N_Port utilization information for N_ports on all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Access Gateway mode must be enabled.

There is a **clear** form of this command, which clears utilization information of RBridges specified. Enabling a port also clears the information.

If an N_port is a trunk slave port, no utilization information is displayed. Instead, the bandwidth is included in the master port of the trunk.

Command Output

The **show ag nport-utilization** command displays the highest bandwidth utilization and associated timestamp associated with each N_port.

Examples

The following command displays utilization information for Access Gateway N_ports on RBridge 1:

```
sw0# show ag nport-utilization rbridge-ID 1
--------------------------------------------------
Name                  : sw0
NodeName              : 10:00:00:05:1e:e5:6d:27
Number of Ports       : 128
IP Address(es)        : 10.17.31.92
Firmware Version      : v5.0.0d
Number of N_Ports(Fi) : 2
Number of VF_Ports    : 2
Policies Enabled      : pg
Disabled
N_Port(Fi) information :
        Port            PortID        Attached PWWN        IP_Addr         VF_Ports
        ------------------------------------------------------------------------------
        Fi 1/0/7       0xa90900  2f:00:00:05:1e:80:31:4f   10.17.31.169    1/1/1, 1/1/2
                highest bandwidth utilization of 11 % recorded at Wed Apr 30 14:07:42 2014

        Fi 1/0/8       0xa90900  2f:00:00:05:1e:80:31:4f   10.17.31.169    None
                trunk slave. bandwidth/traffic added to trunk master
        ------------------------------------------------------------------------------
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

ag, ag enable, clear ag nport-utilization, show ag, show ag map, show ag pg

show ag pg

Displays information on Port Grouping (PG) configured on a switch for Access Gateway (AG) mode.

Syntax

show ag pg [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The command output includes N_Ports and VF_Ports in the group and Port Grouping (PG) modes enabled.

Access Gateway mode must be enabled.

Examples

Following is an example showing port grouping information for RBridge 5:

```
sw0# show ag pg rbridge-id 5
Rbridge-ID 5:
-------------------------------------------------------------------------------------------
PG_ID  PG_Name PG_Mode         N_Ports(Fi)                    VF_Ports
-------------------------------------------------------------------------------
  0    pg0     lb                          5/0/1,5/0/2,5/0/3,5/0/4,         1/5/1,  1/5/2, 1/5/3,
1/5/4,
                                        5/0/5,5/0/6,5/0/7,5/0/8            1/5/5,  1/5/6, 1/5/7,
1/5/8,
                                                1/5/9,  1/5/10, 1/5/11, 1/5/12,
                                                1/5/13, 1/5/14, 1/5/15, 1/5/16,
                                                1/5/17, 1/5/18, 1/5/19, 1/5/20,
                                                1/5/21, 1/5/22, 1/5/23, 1/5/24,
                                                1/5/25, 1/5/26, 1/5/27, 1/5/28,
                                                1/5/29, 1/5/30, 1/5/31, 1/5/32,
                                                1/5/33, 1/5/34, 1/5/35, 1/5/36,
                                                1/5/37, 1/5/38, 1/5/39, 1/5/40,
                                                1/5/41, 1/5/42, 1/5/43, 1/5/44,
                                                1/5/45, 1/5/46, 1/5/47, 1/5/48,
                                                1/5/49, 1/5/50, 1/5/51, 1/5/52,
                                                1/5/53, 1/5/54, 1/5/55, 1/5/56,
                                                1/5/57, 1/5/58, 1/5/59, 1/5/60,


1/5/61, 1/5/62, 1/5/63, 1/5/64
-------------------------------------------------------------------------------
```

Related Commands

pg, show ag, show ag map, show ag nport-utilization

show arp

Displays the ARP cache.

Syntax

show arp [**dynamic**[**summary**]] | *<N>***gigabitethernet** *rbridge-id/slot/port* | **ip** *ip-address* | **static** [**summary**] | **summary** | **ve** *vlan_id*] [**vrf** *name*] [**rbridge-id**[**all**|*rbridge_id*]] | **slot** *slot_no* [[*ip-address*] | [**vrf** *name*] [*ip-address*]]

Parameters

switch_ID
: Unique identifier for a switch (WWN).

all
: Displays ARP information for all RBridge IDs in a cluster.

dynamic
: Displays all the dynamic ARP entries in the ARP table.

*<N>***gigabitethernet**
: Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

  rbridge-id
  : Specifies an RBridge ID.

  slot
  : Specifies a valid slot number.

  port
  : Specifies a valid port number.

ip
: Displays the ARP for a particular next-hop.

  ip-address
  : Displays the ARP information for this next-hop IP address.

slot
: Displays ARP information for a selected slot.

static
: Displays all the static ARP entries in the ARP table.

summary
: Displays a summary of the ARP table (can be used by itself, or succeed the static, dynamic or interface keywords).

ve *vlan_id*
: Specifies the virtual Ethernet (VE) interface to display.

vrf *name*
: Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

show bpdu-drop

Displays information about BPDU guard.

Syntax

show bpdu-drop [**interface** { **port-channel** *num* | <*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

interface
Selects an interface (required).

port-channel *num*
Selects a port channel interface. The number of available channels ranges from 1 through 6144

<*N*>**gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered on any RBridge in a Brocade VCS Fabric.

Related Commands

capture packet interface

show capture packet interface

Displays information about captured packets.

Syntax

show capture packet interface { **all** | *<N>***gigabitethernet** *rbridge-id/slot/port* }

Parameters

all

Selects all interfaces.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays information captured by means of the **capture packet interface** command

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples

```
switch# show capture packet interface all
Packet Capture configured on the following interfaces
 Te 130/0/5 >> ISL
 Te 130/0/6 >> ISL
 Te 130/0/21
 Te 130/0/23
 Te 130/0/24
Frame Received Time : Sat Mar 9 2013 0:57:0:282
 Packet Type         : ELD
 Packet Direction    : TX
 Interface info      : Te 130/0/21
     ETHERNET HEADER
 SrcMAC              : 00:05:33:5e:01:67
 DstMAC              : 03:05:33:5d:f3:fa
 Ethtype             : 0x8100
 Eth Frametype       : 0x33
 VlanID              : 0xfff
     ELD PAYLOAD DETAILS
---------------------------
 Vlan id             : 2
 Src-Rbridgeid       : 130
 Src-Priority        : 5
 Magic Number        : 5103
```

Related Commands

capture packet interface

show cee maps

Displays information on the defined CEE maps. The configuration state is displayed with a list of all of the Layer 2 interfaces bound to the CEE map.

Syntax

show cee maps default

Command Default

The only map name allowed is "default."

Modes

Privileged EXEC mode

Usage Guidelines

Network OS only allows the CEE map named "default."

Examples

To view the CEE map:

```
switch0# show cee maps

CEE Map 'default'
Precedence: 1
Remap Fabric-Priority to Priority 0
Remap Lossless-Priority to Priority 0
Priority Group Table
1:  Weight 40, PFC Enabled, BW% 40
2:  Weight 40, PFC Disabled, BW% 40
3:  Weight 20, PFC Disabled, BW% 20
15.0: PFC Disabled
15.1: PFC Disabled
15.2: PFC Disabled
15.3: PFC Disabled
15.4: PFC Disabled
15.5: PFC Disabled
15.6: PFC Disabled
15.7: PFC Disabled
Priority Table
CoS:    0    1    2    3    4    5    6    7
----------------------------------------
PGID:    2    2    3    1    2    2    2 15.0
```

Related Commands

cee, cee-map (configuration)

show cert-util ldapca

Displays the Lightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate.

Syntax

show cert-util ldapca [**rbridge-id** { *rbridge_id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

To display the LDAP certificate on the switch:

```
switch: show cert-util syslogcacert rbridge-id 3
```

Related Commands

ldap-server host, ldap-server maprole, show running-config ldap-server, username

show cert-util sshkey

Displays the public SSH key for a specified user..

Syntax

show cert-util sshkey user *user_id* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

user *user_id*

The user ID to display.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

A typical output of this command:

```
switch# show cert-util sshkey user testuser

user's public keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAtTCFzC1lfjwV9hjdtqv2ulSvmsmf7q7MS92Ctc3pDje/
YGYJPHVUi8bQX0XAsCAuzdsZL0BlVHdYPO1L4HStuIo8okfn4xLxrazqzwVeeL8p5Zcspf9zK8HmDzNpZ/
OuQ9MvfOuzbseYrovqgYLFGfPvY6vleFXZo61vVncFM7uFzasED9o9JUSBRORhBki7vB0SG69yNn6ADnmpQW6QOu
+nYuZaWXO0QXk2OIB+hidjxSQVAfVLidSIGyfDD0go
+JAE3osxZxwQa5jcorASs4q2Gt4tSYERpvzOsjaAR5YivbmmBTIQWdUuR9Laz8s8VKF4Di9HQ4kE+xyBeAFNvQ==
bmeenaks@blc-10-6
```

To see the output of rbridge-id 3:

```
switch# show cert-util sshkey user testuser rbridge-id 3
```

Related Commands

certutil import sshkey

show cert-util syslogca

Displays the syslog Certification Authority (CA) certificate.

Syntax

show cert-util syslogca [**rbridge-id** { *rbridge_id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

To display the LDAP certificate on the switch:

```
switch# show cert-util ldapca

LDAP CA
```

Related Commands

show running-config ldap-server, ldap-server host, ldap-server maprole, show running-config ldap-server, username

show chassis

displays the Field Replaceable Unit (FRU) header content for each object in the chassis.

Syntax

show chassis [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*

Specifies an RBridge ID for the switch.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local switch and is supported only on the local switch. The output of this command depends on the platforms on which it is executed. Not all information is available for all platforms. In cases where information is not available, the lines are suppressed

Pagination is not supported with this command. Use the "more" parameter to display the output one page at a time.

Command Output

The **show chassis** command displays the Field Replaceable Unit (FRU) header content for each object in the chassis.

Output field	Description
Chassis name and model	For example, BR-VDX6740-48
Chassis backplane revision	
Object type	MM (management module), SFM (switch fabric module), LC (line card), CHASSIS, FAN, POWER SUPPLY, SW CID (chassis ID), WWN (world wide name), or UNKNOWN
Object number	Slot number (for blades), Unit number (for everything else)
Brief description	If the FRU is part of an assembly
FRU header version number or blade version	Header Version: x
Maximum allowed power consumption	Positive value for power supplies; negative value for consumers
Real-time power usage (W)	For FRUs that support real-time power management
Part number (up to 14 characters)	Factory Part Num: xx-xxxxxx-x x
Serial number (up to 12 characters)	Factory Serial Num: xxxxxxxxxx
FRU manufacture date	Manufacture: Day: dd Month: mm Year: yyyy
Date of the last FRU header update	Update: Day: dd Month: mm Year: yyyy
Cumulative time (days) FRU inserted in the chassis with Network OS running	Time Alive :dd days

Output field	Description
Current time (days) since FRU was last powered on or the system restarted	Time Awake: dd days
Airflow direction	
Externally supplied ID (up to 10 characters)	ID: xxxxxxxxxx
Externally supplied part number (up to 20 characters)	Part Num: xxxxxxxxxxxxxxxxxxx
Externally supplied serial number (up to 20 characters)	Serial Num: xxxxxxxxxxxxxxxxxxx
Externally supplied revision number (up to 4 characters)	Revision Num: xxxx

Examples

To display the FRU information on a Brocade VDX switch:

```
switch# show chassis rbridge-id 54

Chassis Name:         BR-VDX6740
Chassis Backplane Revision: 2
switchType: 96
FAN  Unit: 1
Time Awake:             64 days
FAN  Unit: 2
Time Awake:             64 days
POWER SUPPLY  Unit: 1
Header Version:         2
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             0 days
POWER SUPPLY  Unit: 2
Header Version:         2
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             64 days
CHASSIS/WWN  Unit: 1
Header Version:         2
Power Consume Factor:   0
Factory Part Num:       40-1000590-03
Factory Serial Num:     BWU0406G006
Manufacture:            Day: 18  Month:  2  Year: 2011
Update:                 Day:  1  Month:  7  Year: 2012
Time Alive:             594 days
Time Awake:             64 days
```

To display the FRU information on a Brocade VDX 8770-4:

```
switch# show chassis rbridge-id 1

Chassis Name:           BR-VDX8770-4
Chassis Backplane Revision: 2
switchType: 1000
MM  Slot: M1
Blade Version:          3
Power Consume Factor:   -120
Power Usage (Watts):    -43
Factory Part Num:       60-1002179-07
Factory Serial Num:     BVT0329G00D
Manufacture:            Day: 26  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             78 days
Time Awake:             1 days
SFM  Slot: S2
Blade Version:          3
Power Consume Factor:   -150
Power Usage (Watts):    -132
Factory Part Num:       60-1002180-05
Factory Serial Num:     BVU0321G01F
Manufacture:            Day: 39  Month:  5  Year: 17
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             76 days
Time Awake:             1 days
LC  Slot: L1
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-08
Factory Serial Num:     BVV0333G00E
Manufacture:            Day: 17  Month:  8  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             69 days
Time Awake:             1 days
LC  Slot: L2
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-07
Factory Serial Num:     BVV0326G01B
Manufacture:            Day:  5  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             75 days
Time Awake:             1 days
LC  Slot: L3
Blade Version:          3
Power Consume Factor:   -400
Power Usage (Watts):    -261
Factory Part Num:       40-1000573-01
Factory Serial Num:     BTF0333G002
Manufacture:            Day: 48  Month:  8  Year: 17
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             58 days
Time Awake:             1 days
LC  Slot: L4
Blade Version:          3
Power Consume Factor:   -400
Factory Part Num:       60-1002181-07
Factory Serial Num:     BVV0326G01A
Manufacture:            Day:  5  Month:  7  Year: 11
Update:                 Day: 30  Month:  6  Year: 2012
Time Alive:             80 days
Time Awake:             1 days
POWER SUPPLY  Unit: 1
Power Consume Factor:   3000
Factory Part Num:       23-0000135-01
Factory Serial Num:     BMM2J02G003
Manufacture:            Day:  1  Month:  1  Year: 2011
Time Awake:             1 days
ID:                     LPCS
```

```
Part Num:               SP750Z1A
Rework:                 A
POWER SUPPLY  Unit: 2
Power Consume Factor:   3000
Factory Part Num:       23-0000135-01
Factory Serial Num:     BMM2J02G008
Manufacture:            Day:  1  Month:  1  Year: 2011
Time Awake:             1 days
ID:                     LPCS
Part Num:               SP750Z1A
Rework:                 A
FAN  Unit: 1
Power Consume Factor:   -126
Power Usage (Watts):    -19
Factory Part Num:       60-1002130-02
Factory Serial Num:     BYX0320G007
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days
FAN  Unit: 2
Power Consume Factor:   -126
Power Usage (Watts):    -21
Factory Part Num:       60-1002130-02
Factory Serial Num:     BYX0320G011
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days
CID  Unit: 1
Power Consume Factor:   -1
Factory Part Num:       60-1002178-01
Factory Serial Num:     BWF0319G015
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days
CID  Unit: 2
Power Consume Factor:   -1
Factory Part Num:       60-1002178-01
Factory Serial Num:     BWF0319G01Z
Manufacture:            Day:  3  Month:  6  Year: 17
Time Awake:             1 days
Chassis Factory Serial Num: BZA0320G00W
```

Related Commands

show linecard, show mm, show sfm

show cipherset

Displays the current cipherset status for LDAP and SSH.

Syntax

show cipherset

Modes

Privileged EXEC mode

Examples

To display cipherset status on the switch:

```
switch# show cipherset

LDAP Cipher List        : !DH:HIGH:-MD5
SSH Cipher List         : 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
```

Related Commands

cipherset

show class-maps

Displays all the class-maps configured in the system.

Syntax

show class-maps

Modes

Privileged EXEC mode

Related Commands

class-map, policy-map

show cli

Displays all the current CLI settings.

Syntax

show cli

Modes

Privileged EXEC mode

Examples

Typical command output display.

```
switch# show cli
autowizard            false
complete-on-space     false
history               100
idle-timeout          600
ignore-leading-space  false
output-file           terminal
paginate              true
prompt1               \H\M#
prompt2               \H(\m)#
screen-length         73
screen-width          120
service prompt config true
show-defaults         false
terminal              ansi
```

show cli history

Displays the last 512 commands executed on the local node across user sessions.

Syntax

show cli history

Modes

Privileged EXEC mode

show clock

Returns the local time, date, and time zone.

Syntax

show clock [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

The local clock is used.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

If the RBridge ID is not provided, status results default to the local switch (LOCL). If **rbridge-id all** is executed, the command displays the status for all switches in the VCS cluster

This command is currently supported only on the local RBridge.

Examples

To show clock time for all switches in the cluster (Logical chassis cluster mode only):

```
switch# show clock rbridge-id all
```

To show clock time for switch with rbridge-id 16:

```
switch# show clock rbridge-id 16
```

Related Commands

clock set, clock timezone (Privileged EXEC mode), clock timezone (RBridge ID configuration mode), ntp server

show config snapshot

Displays the snapshots present on the switch.

Syntax

show config snapshot [**rbridge-id** { *rbridge-id* | **all** }] [*snapshot-id*]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

snapshot-id

Specifies the name of the snapshot that has been captured. This can be any combination of characters and numbers. The range is from 1 through 50.

Modes

Privileged EXEC mode

Usage Guidelines

A maximum of four snapshots for each RBridge ID can be stored on the switch.

Related Commands

copy snapshot (logical chassis cluster mode)

show copy-support status

Displays the status of the copy support operation.

Syntax

show copy-support status [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The status is indicated by the percentage of completion. On a modular chassis, Use this command to display status information for each module along with the slot number and SS type. NORMAL indicates process is proceeding or completed without errors. FAULTY indicates a faulty blade.

This command is supported only on the local switch.

Examples

To display the support upload status on a Brocade VDX 8770-4:

```
switch# show copy-support status

Slot Name        SS type         Completion Percentage
#########################################################
M1               NORMAL          [100%]
M2               NORMAL          [100%]
L1/0             NORMAL          [100%]
L1/1             NORMAL          [100%]
L2/0             NORMAL          [100%]
L2/1             NORMAL          [100%]
L4/0             NORMAL          [100%]
L4/1             NORMAL          [100%]
```

Related Commands

copy support, copy support-interactive, show support

show dadstatus

Displays the current DHCP auto-deployment (DAD) status output on the switch.

Syntax

show dadstatus

Modes

Privileged EXEC mode

Usage Guidelines

If DAD fails, one of the following errors will show in the output:

1. DHCP auto-deployment failed during DHCP process
2. DHCP auto-deployment failed in sanity check
3. DHCP auto-deployment failed due to same firmware
4. DHCP auto-deployment failed to start firmware download
5. DHCP auto-deployment failed due to firmware download failure

Examples

To display DAD status output on the switch:

```
sw0# show dadstatus
   [1] : Thu Aug 15 23:22:50 GMT 2013
   DHCP Auto-deployment enabled

   [2] : Thu Aug 15 23:27:20 GMT 2013
   DHCP Auto-deployment started firmwaredownload

   [3] : Thu Aug 15 23:38:57 GMT 2013
   DHCP Auto-deployment succeeded

sw0# show dadstatus
   [1] : Fri Aug 16 12:02:44 GMT 2013
   DHCP Auto-deployment enabled

   [2] : Fri Aug 16 12:10:03 GMT 2013
   DHCP Auto-deployment failed in sanity check.
```

Related Commands

firmware download, firmware download logical-chassis, dhcp auto-deployment enable

show debug dhcp packet

Displays the DHCP packet capture configuration for interfaces configured for DHCP packet capturing.

Syntax

show debug dhcp packet

Modes

Privileged EXEC mode

Examples

```
sw0# show debug dhcp packet

%  DHCP  protocol  RCV debug is enabled on interface Te 3/18
%  DHCP  protocol  TX debug is enabled on interface Te 3/18
PCAP Buffer Configuration for Vrf ID 0: Buffer Type is Linear and BufferSize is 2056
```

Related Commands

debug dhcp packet buffer interface

show debug dhcp packet buffer

Displays DHCP packets saved in the DHCP packet capture buffer for all VRF IDs.

Syntax

show debug dhcp packet buffer

Modes

Privileged EXEC mode

Examples

The following command displays buffer content for all VRF IDs.

```
sw0# show debug dhcp packet buffer
Protocol Type       : DHCP
Packet Flow         : RX
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 1 (DHCP-Discover)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 2 (DHCP-Offer)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : RX
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 3 (DHCP-Request)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 5 (DHCP-Ack)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
```

```
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
```

Related Commands

debug dhcp packet buffer clear, debug dhcp packet buffer interface

show debug ip bgp all

Displays all BGP4 debug options that are enabled.

Syntax

show debug ip bgp all

Modes

Privileged EXEC mode

Examples

```
switch# show debug ip bgp all
```

show debug ip igmp

Displays the IGMP packets received and transmitted, as well as related events.

Syntax

show debug ip igmp

Modes

Privileged EXEC mode

show debug ip pim

Displays the current state of the Protocol Independent Multicast (PIM) debug flags.

Syntax

show debug ip pim

Modes

Privileged EXEC mode

Examples

A typical output of this command.

```
switch# show debug ip pim

PIM debugging status:
--------------------------
add-del-oif  : off
bootstrap    : off
group        : off
join-prune   : on
nbr-change   : off
packets      : off
parent       : off
regproc      : off
route-change : off
rp           : off
source       : off
--------------------------
```

show debug ipv6 packet

Displays IPv6 packets captured through the packet capture utility on an interface or all interfaces, as well as the packet capture configuration on the switch.

Syntax

show debug ipv6 packet [**buffer** [**all** | **interface** [*<N>* **gigabitethernet** *rbridge-id/slot/port*| **ve** *vlan_id*] [**rx** | **tx**]

Parameters

buffer
Specifies IPv6 packets.

all
Specifies all interfaces.

interface
Specifies an interface.

<N> **gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve*vlan_id*
Specifies a virtual Ethernet interface.

Command Default

None

Modes

Privileged EXEC mode

Examples

To display the current PCAP configuration on the switch:

```
switch# show debug ipv6 packet
```

To display IPv6 packets captured on all interfaces:

```
switch# show debug ipv6 packet buffer all
```

To display IPv6 packets captured on a specific interface:

```
switch# show debug ipv6 packet buffer int te 54/0/1
```

History

Release version	Command history
5.0.0	This command was introduced.

show debug lacp

Displays the status of LACP debugging flags on the switch.

Syntax

show debug lacp

Modes

Privileged EXEC mode

show debug lldp

Displays the LLDP debugging status on the switch.

Syntax

show debug lldp

Modes

Privileged EXEC mode

Examples

To display the LLDP debugging status on the switch:

```
switch# show debug lldp

LLDP debugging status:
Interface te0/0    : Transmit Receive  Detail
```

show debug spanning-tree

Displays the status of STP debugging flags on the switch.

Syntax

show debug spanning-tree

Modes

Privileged EXEC mode

show debug udld

Shows UDLD debug status on the switch.

Syntax

show debug udld

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the unidirectional link detection (UDLD) protocol debug status of the switch. The status reflects the bugging you set with the **debug udld** command.

Related Commands

protocol udld, debug udld packet

show debug vrrp

Displays the status of VRRP debugging flags on the switch.

Syntax

show debug vrrp

Modes

Privileged EXEC mode

Usage Guidelines

This command is for VRRP and VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples

If you run this command and the debug parameter has already been set to debug all VRRP events, the following is displayed:

```
switch# show debug vrrp

VRRP event debugging is on
```

show defaults threshold

Displays the default thresholds for environmental and alert values for Ethernet interfaces, login, Telnet security monitoring, and SFPs.

Syntax

show defaults threshold [**interface type Ethernet** | **security** | **sfp**]

Parameters

interface type Ethernet
Thresholds for all Ethernet interfaces.

security
Thresholds for login and Telnet monitoring.

sfp
Thresholds for the following SFP types:

1 GLR

1 GSR

10 GLR

10 GSR

10 GUSR

QSFP

Modes

Privileged EXEC mode

Usage Guidelines

These thresholds can be changed by means of the **threshold-monitor** command.

Examples

The following example illustrates default interface thresholds:

```
switch# show defaults threshold interface type Ethernet
Type: GigE-Port
+------------+----------------------+----------------------+--------+--------+
|            |    High Threshold    |    Low Threshold     | Buffer | Time   |
| Area       |Value | Above | Below |Value | Above | Below | Value  | Base   |
|            |      | Action| Action|      | Action| Action|        |        |
+------------+------+-------+-------+------+-------+-------+--------+--------+
| MTC        |  300 | none  | none  |    12| none  | none  |       0| minute |
+------------+------+-------+-------+------+-------+-------+--------+--------+
| CRCAlign   |  300 | none  | none  |    12| none  | none  |       0| minute |
+------------+------+-------+-------+------+-------+-------+--------+--------+
| Symbol     |    5 | none  | none  |     0| none  | none  |       0| minute |
+------------+------+-------+-------+------+-------+-------+--------+--------+
| IFG        |  100 | none  | none  |     5| none  | none  |       0| minute |
+------------+------+-------+-------+------+-------+-------+--------+--------+
MTC - Missing Termination Character
```

The following example illustrates security thresholds:

```
sw0# show defaults threshold security
+------------+----------------------+----------------------+--------+--------+
|            |    High Threshold    |    Low Threshold     | Buffer | Time   |
| Area       |Value | Above | Below |Value     | Below     | Value  | Base   |
|            |      | Action| Action|          | Action    |        |        |
+------------+------+-------+-------+----------+-----------+--------+--------+
| Telnet     |    2 | raslog | none |         1| none      |       0| minute |
+------------+------+-------+-------+----------+-----------+--------+--------+
| Login      |    2 | raslog | none |         1| none      |       0| minute |
+------------+------+-------+-------+----------+-----------+--------+--------+
```

Related Commands

show threshold monitor, threshold-monitor cpu

show default-vlan

Displays the current default VLAN value.

Syntax

show default-vlan

Modes

Privileged EXEC mode

Related Commands

show running reserved-vlan, reserved-vlan

show dpod

Displays Dynamic Ports on Demand (DPOD) licensing.

Syntax

show dpod [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged Exec mode

Usage Guidelines

This command has no effect on Brocade VDX 6710 and VDX 8770 switches. These switches do not support the Dynamic POD feature.

In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.

Examples

```
switch# show dpod
rbridge-id: 15
48 10G ports are available in this switch
4 40G ports are available in this switch
10G Port Upgrade license is installed
40G Port Upgrade license is installed
Dynamic POD method is in use
32 10G port assignments are provisioned for use in this switch:
24 10G port assignments are provisioned by the base switch license
8 10G port assignments are provisioned by the Port Upgrade license
1 10G port is assigned to installed licenses:
1 10G port is assigned to the base switch license
0 10G ports are assigned to the Port Upgrade license
10G ports assigned to the base switch license:
15/0/12
10G ports assigned to the Port Upgrade license:
None
10G ports not assigned to a license:
15/0/1, 15/0/2, 15/0/3, 15/0/4, 15/0/5, 15/0/6, 15/0/7, 15/0/8, 15/0/9,
15/0/10
15/0/11, 15/0/13, 15/0/14, 15/0/15, 15/0/16, 15/0/17, 15/0/18, 15/0/19,
15/0/20, 15/0/21
15/0/22, 15/0/23, 15/0/24, 15/0/25, 15/0/26, 15/0/27, 15/0/28, 15/0/29,
15/0/30, 15/0/31
15/0/32, 15/0/33, 15/0/34, 15/0/35, 15/0/36, 15/0/37, 15/0/38, 15/0/39,
15/0/40, 15/0/41
15/0/42, 15/0/43, 15/0/44, 15/0/45, 15/0/46, 15/0/47, 15/0/48
31 10G license reservations are still available for use by unassigned ports
16 40G port assignments are provisioned for use in this switch:
0 40G port assignments are provisioned by the base switch license
2 40G port assignments are provisioned by the Port Upgrade license
1 40G port is assigned to installed licenses:
836 Network OS Command Reference
53-1003226-01
5 show dpod
0 40G ports are assigned to the base switch license
1 40G ports are assigned to the Port Upgrade license
40G ports assigned to the base switch license:
None
40G ports assigned to the Port Upgrade license:
15/0/49
40G ports not assigned to a license:
15/0/50, 15/0/51, 15/0/52
3 40G license reservations are still available for use by unassigned ports
```

Related Commands

show running-config dpod

show diag burninerrshow

Displays the error messages that are stored in the nonvolatile storage on the slot during the POST and system verification processes.

Syntax

show diag burninerrshow [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The error messages are updated when there is a POST failure or a systemVerification failure. To display burn-in errors from the switch:

```
switch# show diag burninerrshow rbridge-id 1

errLog for slot M2
errLog is empty for slot M2
errLog for slot S1
errLog is empty for slot S1
errLog for slot S2
errLog is empty for slot S2
errLog for slot S3
errLog is empty for slot S3
errLog for slot L4
errLog is empty for slot L4
rbridgeId 1
```

Related Commands

diag burninerrclear, diag clearerror, show diag burninstatus

show diag burninerrshowerrLog

Displays the error log messages that are stored in the nonvolatile storage on the slot during the POST and system verification processes.

Syntax

show diag burninerrshowerrLog [**slot** *slot-id*]

Parameters

slot *slot_id*

Specifies the slot ID. This is mandatory for slot-based systems only.

Modes

Privileged EXEC mode

Examples

The error messages are updated when there is a POST failure or a systemVerification failure. To display the error log messages on the slot:

```
switch# show diag burninerrshowerrLog
Log for slot M1errLog is empty for slot M1errLog for slot S12012/06/03-07:11:17:038992, [DIAG-5004], 0,
M1, INFO, chassis, DIAG-MANUAL4 " S1 verify: Starting run Sun Jun 3 07:11:14 PDT 2012 "Err# 0140045
0300:101:000:001:0:20: , OID:0x430c0000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:31:02:766063, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S1 verify:
TESTED stat PASSED 5 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 53 sec (0:18:53)"Err# 0140045
0300:101:000:001:0:20: , OID:0x430c0000, iobuf.c, lineerrLog for slot S22012/06/03-07:11:16:618653,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S2 verify: Starting run Sun Jun 3 07:11:13 PDT 2012
"Err# 0140045 0400:101:000:001:0:20: , OID:0x43100000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:30:39:636631, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S2 verify:
TESTED stat PASSED 5 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 58 sec (0:18:58)"Err# 0140045
0400:101:000:001:0:20: , OID:0x43100000, iobuf.c, lineerrLog for slot S32012/06/03-07:11:12:838561,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S3 verify: Starting run Sun Jun 3 07:11:09 PDT 2012
"Err# 0140045 0500:101:000:001:0:20: , OID:0x43140000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:30:35:017964, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " S3 verify:
TESTED stat PASSED 5 cmds in 1 runs Therm 10 Vib 2 in 0 hr 19 min 4 sec (0:19:4)"Err# 0140045
0500:101:000:001:0:20: , OID:0x43140000, iobuf.c, line:errLog for slot L12012/06/03-07:11:18:678484,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L1 verify: Starting run Sun Jun 3 07:11:15 PDT 2012
"Err# 0140045 0700:101:000:001:0:20: , OID:0x431c0000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:30:56:177298, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L1 verify:
TESTED stat PASSED 8 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 44 sec (0:18:44)"Err# 0140045
0700:101:000:001:0:20: , OID:0x431c0000, iobuf.c, lineerrLog for slot L22012/06/03-07:11:18:678576,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L2 verify: Starting run Sun Jun 3 07:11:15 PDT 2012
"Err# 0140045 0800:101:000:001:0:20: , OID:0x43200000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:30:40:774116, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L2 verify:
TESTED stat PASSED 8 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 41 sec (0:18:41)"Err# 0140045
0800:101:000:001:0:20: , OID:0x43200000, iobuf.c, lineerrLog for slot L32012/06/03-07:11:17:097345,
[DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L3 verify: Starting run Sun Jun 3 07:11:14 PDT 2012
"Err# 0140045 0900:101:000:001:0:20: , OID:0x43240000, iobuf.c, line: 648, comp:insmod, ltime:
2012/06/03-07:2012/06/03-07:19:29:651740, [DIAG-5046], 0, M1, ERROR, chassis, L3:portLoopbackTest
FAILED. Err -2, OID:0x43240000, diag_mercury_mm, line: 543, comp:diag, ltime:
2012/06/03-07:19:29:6516992012/06/03-07:29:52:276612, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 "
L3 verify: TESTED stat FAILED 8 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 34 sec (0:18:34)"Err#
0140045 0900:101:000:001:0:20: , OID:0x43240000, iobuf.c, lineerrLog for slot
L42012/06/03-07:11:17:385343, [DIAG-5004], 0, M1, INFO, chassis, DIAG-MANUAL4 " L4 verify: Starting run
Sun Jun 3 07:11:15 PDT 2012 "Err# 0140045 0A00:101:000:001:0:20: , OID:0x43280000, iobuf.c, line: 648,
comp:insmod, ltime:2012/06/03-07:2012/06/03-07:30:27:647391, [DIAG-5004], 0, M1, INFO, chassis, DIAG-
MANUAL4 " L4 verify: TESTED stat PASSED 8 cmds in 1 runs Therm 10 Vib 2 in 0 hr 18 min 55 sec
(0:18:55)"Err# 0140045 0A00:101:000:001:0:20: , OID:0x43280000, iobuf.c, linerbridgeId 233M4_237_233#
```

Related Commands

diag burninerrclear, diag clearerror, show diag burninstatus

show diag burninstatus

Displays the diagnostics burn-in status or system verification status stored in the nonvolatile storage memory in the switch.

Syntax

show diag burninstatus [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To display the diagnostics burn-in status:

```
switch# show diag burninstatus

DiagID  State           Status  Run     Cmd     TotCmds PID     Script  SlotID
1       COMPLETE_TESTED PASS    1       8       8       23163   verify  L1
2       COMPLETE_TESTED PASS    1       8       8       23311   verify  L2
6       COMPLETE_TESTED PASS    1       5       5       23465   verify  S2
7       COMPLETE_TESTED PASS    1       5       5       23618   verify  S3
8       COMPLETE_TESTED PASS    1       5       5       23787   verify  S4
9       COMPLETE_TESTED PASS    1       5       5       23976   verify  S5
10      COMPLETE_TESTED PASS    1       5       5       24156   verify  S6
12      COMPLETE_TESTED PASS    1       8       8       24388   verify  L6
14      COMPLETE_TESTED PASS    1       8       8       24692   verify  L8
rbridgeId 1
```

Related Commands

diag burninerrclear, diag clearerror, show diag burninerrshow

show diag post results

Displays either the brief results or detailed information of the power-on self-test (POST) executed on the switch.

Syntax

show diag post results { **brief** | **detailed** } [**rbridge-id** *rbridge-id*] [**slot** *slot-id*]

Parameters

brief | **detailed**

Specifies whether the POST passed or failed (brief) or displays detailed status with the register dump when a POST fails (detailed).

rbridge-id *rbridge-id*

Specifies an RBridge ID.

slot *slot_id*

Specifies the slot ID. This is mandatory for slot-based systems only.

Modes

Privileged EXEC mode

Examples

To display brief POST results (whether the POST passed or failed):

```
switch# show diag post results brief slot L4

POST1:Slot L4 turboramtest PASSED (exit_status 0).
POST1:Slot L4 Script PASSED with exit_status of 0 Thu Jan 1 00:04:36 GMT 1970 took (0:0:47)
POST2:Slot L4 portloopbacktest PASSED (exit_status 0).
POST2:Slot L4 prbstest PASSED (exit_status 0).
POST2:Slot L4 Script PASSED with exit_status of 0 Thu Jan 1 00:05:52 GMT 1970 took (0:1:15)
rbridgeId 1
switch# show diag post results detailed slot S1

POST1:Slot S1 Started running Thu Jan 1 00:02:46 GMT 1970
POST1:Slot S1 Running diagclearerror
POST1:Slot S1 Running diagsetup
POST1:Slot S1 Test #1 - Running turboramtest
Running turboramtest...
:
<..cut..>
:
POST1:Slot S1 ********** Slot S1 POST Summary **********
POST1:Slot S1 Completed 1 Diagnostic test:
POST1:Slot S1 Script PASSED with exit_status of 0 Thu Jan 1 00:02:53 GMT 1970 took (0:0:7)
POST2:Slot S1 Started running Thu Jan 1 00:02:58 GMT 1970
POST2:Slot S1 Running diagclearerror
POST2:Slot S1 Test #1 - Running portloopbacktest
Running portloopbacktest...
:
<..cut..>
:
POST2: ********** Slot S1 POST Summary **********
POST2:Slot S1 Completed 2 Diagnostic test:
POST2:Slot S1 Script PASSED with exit_status of 0 Thu Jan 1 00:03:35 GMT 1970 took (0:0:37)
rbridgeId 1
```

Related Commands

diag post enable

show diag setcycle

Displays the current system verification test parameters.

Syntax

show diag setcycle [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To display current values used in system verification:

```
switch# show diag setcycle

CURRENT - KEYWORD           : DEFAULT
 1      - number_of_runs    :  1
 2      - min_lb_mode       :  2
 1      - tbr_passes        :  1
 16     - plb_nframes       : 16
 1      - pled_passes       :  1
rbridgeId 1
```

Related Commands

diag setcycle

show diag status

Displays the currently diagnostic test status on one or all slots in the system.

Syntax

show diag status [**rbridge-id** *rbridge-id*] [**slot** *slot-id*]

Command Default

If an RBridge ID is not specified, diagnostic tests for all blades in the system are displayed.

Parameters

rbridge-id *rbridge-id*

Specifies an RBridge ID.

slot *slot_id*

Specifies the slot ID. This is mandatory for slot-based systems only.

Modes

Privileged EXEC mode

Examples

To automatically display current diagnostic status in the console:

```
switch# show diag status rbridge-id 1

Slot M2 [2]: DIAG runs 'NONE'
Slot S1 [3]: DIAG runs 'NONE'
Slot S2 [4]: DIAG runs 'NONE'
Slot S3 [5]: DIAG runs 'NONE'
Slot L4 [10]: DIAG runs 'NONE'
rbridgeId 1
```

To display the diagnostic status when POST is running on the LC or SFM using the slot ID:

```
switch# show diag status rbridge-id 233 slot L1

Slot L1 [7]:DIAG runs 'turboramtest'
rbridgeId 233
switch# show diag status slot L1

Slot L1 [7]: DIAG runs 'turboramtest'
rbridgeID 233
```

Related Commands

show diag post results

show dot1x

Displays the overall state of dot1x on the system.

Syntax

show dot1x

Modes

Privileged EXEC mode

Examples

To display the state of dot1x on the system:

```
switch# show dot1x

802.1X Port-Based Authentication Enabled
PAE Capability:           Authenticator Only
Protocol Version:         2
Auth Server:              RADIUS
RADIUS Configuration
--------------------
Position:                 1
Server Address:           172.21.162.51
Port:                     1812
Secret:                   sharedsecret
Position:                 2
Server Address:           10.32.154.113
Port:                     1812
Secret:                   sharedsecret
```

show dot1x all

Displays detailed dot1x information for all of the ports.

Syntax

show dot1x all

Modes

Privileged EXEC mode

Examples

To display detailed dot1x information for all of the ports:

```
switch# show dot1x all

802.1X Port-Based Authentication Enabled
PAE Capability:           Authenticator Only
Protocol Version:         2
Auth Server:              RADIUS
802.1X info for interface te0/16
----------------------------------
Port Control:             Auto
Port Auth Status:         Unauthorized
Protocol Version:         2
ReAuthentication:         Disabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         3600 seconds
PAE State:                Connected
BE State:                 Invalid
Supplicant Name:          --
Supplicant Address:       0000.0000.0000
Current Id:               1
Id From Server:           0
```

show dot1x diagnostics interface

Displays all diagnostics information for the authenticator associated with a port.

Syntax

show dot1x diagnostics interface [*<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display all diagnostics information for the authenticator associated with a port:

```
switch# show dot1x diagnostics interface tengigabitethernet 5/0/16

802.1X Diagnostics for interface te5/0/16
 authEnterConnecting: 0
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 0
 authSuccessWhileAuthenticating: 0
 authTimeoutWhileAuthenticating: 0
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 0
 BackendAccessChallenges: 0
 BackendOtherrequestToSupplicant: 0
 BackendAuthSuccess: 0
 BackendAuthFails: 0
```

show dot1x interface

Displays the state of a specified interface.

Syntax

show dot1x interface [<*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

To display the state of the 10-gigabit Ethernet interface 0/16:

```
switch# show dot1x interface tengigabitethernet 5/0/16

Dot1x Global Status:      Enabled
802.1X info for interface te5/0/16
-----------------------------------
Port Control:             Auto
Port Auth Status:         Unauthorized
Protocol Version:         2
ReAuthentication:         Disabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         3600 seconds
PAE State:                Connected
BE State:                 Invalid
Supplicant Name:          --
Supplicant Address:       0000.0000.0000
Current Id:               1
Id From Server:           0
```

show dot1x session-info interface

Displays all statistical information of an established session.

Syntax

show dot1x session-info interface [<*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display all statistical information of the established session:

```
switch# show dot1x session-info interface tengigabitethernet 0/16

802.1X Session info for te0/16
------------------------------
User Name:                testuser
Session Time:             3 mins 34 secs
Terminate Cause:          Not terminated yet
```

show dot1x statistics interface

Displays the statistics of a specified interface.

Syntax

show dot1x statistics interface [*<N>*__gigabitethernet__ *rbridge-id/slot/port*]

Parameters

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, __tengigabitethernet__ specifies a 10-Gb Ethernet port). The use of __gigabitethernet__ without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The __gigabitethernet__ *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

To display the statistics for the 10-gigabit Ethernet interface 22/0/16:

```
switch# show dot1x statistics interface tengigabitethernet 22/0/16

802.1X statistics for interface te22/0/16
  EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 2 - EAP Response Frames Rx: 10
  EAP Req/Id Frames Tx: 35 - EAP Request Frames Tx: 0
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000
```

show dpod

Displays Dynamic Ports on Demand (POD) license information.

Syntax

show dpod [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

This command is executed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The Dynamic POD feature is not supported on Brocade VDX 8770 switches.

Examples

To display Dynamic POD assignment information:

```
switch# show dpod
rbridge-id: 1
24 ports are available in this switch
1 POD license is installed
Dynamic POD method is in use
24 port assignments are provisioned for use in this switch:
16 port assignments are provisioned by the base switch license
8 port assignments are provisioned by the first POD license
* 0 more assignments are added if the second POD license is installed
21 ports are assigned to installed licenses:
16 ports are assigned to the base switch license
5 ports are assigned to the first POD license
Ports assigned to the base switch license:
Te 1/0/1, Te 1/0/10, Te 1/0/11, Te 1/0/12, Te 1/0/13, Te 1/0/14, Te 1/0/15,
Te 1/0/16, Te 1/0/17, Te 1/0/18, Te 1/0/19, Te 1/0/20, Te 1/0/21, Te 1/0/22, Te
1/0/23, Te 1/0/24
Ports assigned to the first POD license:
Te 1/0/5, Te 1/0/6, Te 1/0/7, Te 1/0/8, Te 1/0/9
Ports assigned to the second POD license:
None
Ports not assigned to a license:
Te 1/0/2, Te 1/0/3, Te 1/0/4
3 license reservations are still available for use by unassigned ports
```

Related Commands

dpod, show running-config dpod

show edge-loop-detection detail

Displays ELD detailed information for the entire node.

Syntax

show edge-loop-detection detail [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

ELD configuration mode

Usage Guidelines

This functionality detects Layer 2 loops only.

If no rbridge ID is specified, ELD data on the particular node is displayed.

If an rbridge ID is specified, ELD data for the node with that particular rbridge-id is displayed.

If all rbridge IDs are specified, ELD data from all the nodes in the cluster is displayed.

Examples

```
switch(conf-if-te-119/0/1)# do show edge-loop-detection detail
Number of edge-loop-detection instances enabled: 1
        Data for Rbridge-id: 119
        Total_instances: 1
        Eld-mac: 03:05:33:65:1b:ec
        Data for interface: te0/1
        Eld-instance no. (enabled for VLANs): 1
        Priority: 128   If_status: 1
        Shutdown-vlan: 0        Vlag-master-id: 0       Age-left: 31913 mins
        Port-type : 3   pvid_frame_type: 2      Brcd-agg-type: 0
        Eld stats:      Tx      Rx
                        42      0
        Enabled for Vlan-id: 10
        Send-untagged: 0
        time-rxlimit : 0
        Vlan stats:     Tx      Rx
                        42      0
switch(conf-if-te-119/0/1)#
```

Related Commands

edge-loop-detection vlan, hello-interval, pdu-rx-limit, protocol edge-loop-detection, shutdown-time

show edge-loop-detection globals

Displays ELD global configuration values for status, disabled ports, and resource.

Syntax

show edge-loop-detection globals

Modes

Privileged EXEC mode

ELD configuration mode

Usage Guidelines

The command output displays the PDU receive limit, shutdown time, and hello time.

This command detects Layer 2 loops only.

Examples

To view the ELD global configuration values:

```
switch# show edge-loop-detection globals

Edge-loop-detection global configuration values are as below:
PDU receive limit (packets):    1
Shutdown-time (minutes):        0
Hello-time (msec):              1000
```

Related Commands

edge-loop-detection vlan, hello-interval, pdu-rx-limit, protocol edge-loop-detection, shutdown-time

show edge-loop-detection interface

Displays ELD configuration settings and status for a specific interface and to view the number of packets received and transmitted.

Syntax

show edge-loop-detection interface *interface-type interface-id*

show edge-loop-detection interface { *<N>*__gigabitethernet__ *rbridge-id/slot/port* | **port-channel** *number* }

Parameters

interface-type
Specifies an interface type.

interface-id
Specifies an interface ID.

*<N>*__gigabitethernet__
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, __tengigabitethernet__ specifies a 10-Gb Ethernet port). The use of __gigabitethernet__ without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies the interface is a port-channel. Valid values range from 1 through 6144.

Modes

Privileged EXEC mode

ELD configuration mode

Usage Guidelines

This functionality detects Layer 2 loops only.

Examples

To view the ELD status for a specific interface:

```
switch(conf-if-te-7/0/5)# do show edge-loop-detection interface tengigabitethernet 7/0/5

Number of eld instances: 1
Enabled on VLANs:       100
Priority:               128
Interface status:       UP
Auto enable in:         Never
Packet Statistics:
vlan            sent            rcvd
100             100               0
switch(conf-if-te-7/0/5)# do show edge-loop-detection rbridge-id 7

Number of edge-loop-detection instances enabled: 1
Interface: 7/0/5
------------------------
        Enabled on VLANs: 100
        Priority:       128
        Interface status: UP
        Auto enable in: Never
```

Related Commands

clear edge-loop-detection, edge-loop-detection port-priority, edge-loop-detection vlan, protocol edge-loop-detection, shutdown-time

show edge-loop-detection rbridge-id

Displays ELD status information for a specific RBridge, including the ports that ELD has disabled..

Syntax

show edge-loop-detection rbridge-id { *rbridge-id* | **all** }

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

This functionality detects Layer 2 loops only.

For each interface on which ELD is enabled, this command shows the enabled VLANs, the ELD port priority, the up/down status of the interface, and time to the next automatic port re-enable. The command includes display of disabled interfaces.

If a single rbridge ID is specified, ELD data for the node with that particular rbridge-id is displayed.

If all rbridges are specified, ELD data from all the nodes in the cluster is displayed.

Examples

To view the ELD status:

```
switch# show edge-loop-detection rbridge-id 7

Number of edge-loop-detection instances enabled: 1
Interface: 7/0/5
------------------------
        Enabled on VLANs: 100
        Priority:       128
        Interface status: UP
        Auto enable in: Never
```

Related Commands

clear edge-loop-detection, edge-loop-detection port-priority, edge-loop-detection vlan, shutdown-time

show environment fan

Displays fan status information.

Syntax

show environment fan [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Command Output

The command displays the following information:

Output field	Description
OK	Fan is functioning correctly at the displayed speed (RPM).
absent	Fan is not present.
below minimum	Fan is present but rotating too slowly or stopped.
above maximum	Fan is rotating too quickly.
unknown	Unknown fan unit installed.
faulty	Fan has exceeded hardware tolerance and has stopped. In this case, the last known fan speed is displayed.
Airflow direction	Port side intake or Port side exhaust. This value is not applicable to modular chassis.
speed	Fan RPM.

Examples

To display the fan status information on a Brocade VDX 8770-4:

```
switch# show environment fan

Fan 1 is Ok, speed is 2057 RPM
Fan 2 is Ok, speed is 2009 RPM
```

Related Commands

show environment history, show environment power, show environment sensor, show environment temp

show environment history

Displays the field-replaceable unit (FRU) history log.

Syntax

show environment history [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The history log records insertion and removal events for field-replaceable units (FRUs), such as blades, power supplies, fans, and world wide name (WWN) or chassis ID (CID) cards. The type of FRU supported depends on the hardware platform.

Command Output

The **show environment history** command displays the following information:

Output field	Description
Object type	On standalone platforms: FAN, POWER SUPPLY, WWN (WWN card), or UNKNOWN. On modular platforms: CHASSIS, CID (chassis ID card), FAN, POWER SUPPLY, SW BLADE (port blade), MM[1–2] (management module), SFM (switch fabric module), LC[1–8] (line card) or UNKNOWN.
Object number	Displays the slot number for blades. Displays the unit number for all other object types.
Event type	Displays Inserted, Removed, or Invalid.
Time of the event	Displays the date in the following format: Day Month dd hh:mm:ss yyyy.
Factory Part Number	Displays the part number (xx-yyyyyyy-zz) or Not available.
Factory Serial Number	Displays the FRU serial number (xxxxxxxxxxx) or Not available.

Examples

To display the FRU history on a Brocade VDX 8770-4

```
switch# show environment history

CID  Unit 2             Inserted at Tue Sep  6 22:40:27 2011
Factory Part Number:    40-1000592-01
Factory Serial Number:  BVW0311G00K
SFM  Slot 3             Inserted at Tue Sep  6 22:41:47 2011
Factory Part Number:    60-1002180-05
Factory Serial Number:  BVU0321G00N
LC  Slot 9              Inserted at Tue Sep  6 22:41:48 2011
Factory Part Number:    60-1002181-07
Factory Serial Number:  BVV0326G019
LC  Slot 10             Inserted at Tue Sep  6 22:41:50 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F
MM  Slot 1              Inserted at Tue Sep  6 22:41:50 2011
Factory Part Number:    60-1002179-07
Factory Serial Number:  BVT0329G00B
SFM  Slot 4             Inserted at Wed Sep  7 00:01:44 2011
Factory Part Number:    60-1002180-06
Factory Serial Number:  BVU0329G00B
LC  Slot 10             Removed at Mon Sep 12 19:04:58 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F
LC  Slot 10             Inserted at Mon Sep 12 19:12:21 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G01F
LC  Slot 1              Inserted at Mon Sep 12 19:19:52 2011
Factory Part Number:    40-100522-02
Factory Serial Number:  BSX0312G00B
(Output truncated)
```

Related Commands

show environment fan, show environment power, show environment sensor, show environment temp

show environment power

Displays the type and current status of the switch power supply.

Syntax

show environment power [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Command Output

The **show environment power** command displays the following information:

Output field	Description
OK	Power supply is functioning correctly.
absent	Power supply is not present.
unknown	Unknown power supply unit is installed.
predicting failure	Power supply is present but predicting failure. Replace the power supply as soon as possible.
faulty	Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).
Airflow	Direction of fan air flow (not applicable to modular chassis).

Examples

To display the power supply status:

```
switch# show environment power

Power Supply #1 is OK
LPCS      F@ 11/01/18 type: AC V165.2 3000W
Power Supply #2 is OK
LPCS      F@ 11/01/18 type: AC V165.2 3000W
Power Supply #3 is absent
Power Supply #4 is absent
Power Supply #1 is faulty
```

Related Commands

show environment fan, show environment history, show environment sensor, show environment temp

show environment sensor

Displays the environment sensor status.

Syntax

show environment sensor [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The command output displays the current temperature, fan, and power supply status readings from sensors located on the switch. Refer to the **show environment power** command for an explanation of the power supply status values.

Examples

To display the sensor readings on the switch:

```
switch# show environment sensor

sensor  1: (Temperature ) is Ok, value is 36 C
sensor  2: (Temperature ) is Ok, value is 40 C
sensor  3: (Temperature ) is Ok, value is 32 C
sensor  4: (Fan         ) is Absent
sensor  5: (Fan         ) is Ok,speed is 7345 RPM
sensor  6: (Power Supply) is Absent
sensor  7: (Power Supply) is Ok
```

Related Commands

show environment fan, show environment history, show environment power, show environment temp

show environment temp

Displays environment temperature.

Syntax

show environment temp [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Command Output

The **show environment temp** command displays the following information:

Output field	Description
Sensor ID	
Slot number	(On modular chassis only)
Sensor state	
Temperature	Displayed in both Centigrade and Fahrenheit.

Examples

To display the temperature readings on a Brocade VDX switch:

```
switch# show environment temp

Sensor  State           Centigrade     Fahrenheit
  ID
================================================
  1     Ok                  36             96
  2     Ok                  40            104
  3     Ok                  32             89
```

Related Commands

show environment fan, show environment history, show environment power, show environment sensor

show fabric all

Displays the Brocade VCS Fabric membership information.

Syntax

show fabric all

Modes

Privileged EXEC mode

Usage Guidelines

If the switch is initializing or is disabled, the message "Local Switch disabled or fabric is re-building" is displayed. If the fabric is reconfiguring, some or all switches may not be displayed.

Command Output

The **show fabric all** command displays the following information:

Output field	Description
VCS ID	VCS ID of the switch
Config Mode VCS mode of the switch.	For fabric cluster mode, "Local-Only" is displayed.
Rbridge-id	The RBridge ID of the switch.
WWN	The switch World Wide Name.
IP Address	The switch Ethernet IP address.
Name The switch symbolic name.	An arrow (>) indicates the principal switch. An asterisk (*) indicates the switch on which the command is entered.

Examples

```
switch# show fabric all

Config Mode: Local-Only
Rbridge-id   WWN                       IP Address         Name
-------------------------------------------------------------------------
1            10:00:00:05:1E:CD:44:6A   10.17.87.144       "RB1"
2            10:00:00:05:1E:CD:42:6A   10.17.87.145       "RB2"*
3            10:00:00:05:1E:CD:55:6A   10.17.87.155       "RB3"
4            10:00:00:05:1E:CD:42:EA   10.17.87.156       "RB4"
5            10:00:00:05:1E:CD:52:6A   10.17.87.157       "RB5"
6            10:00:00:05:1E:CD:53:6A   10.17.87.158       "RB6"
10           10:00:00:05:33:13:6A:BE   10.17.87.169       "RB10"
11           10:00:00:05:1E:CD:38:6A   10.17.86.240       "RB11"
12           10:00:00:05:1E:CD:3F:EA   10.17.86.241      >"RB12-a"
The Fabric has 9 Rbridge(s)
```

The angle bracket (>), as shown with RBridge ID 12-a, indicates the principal switch. The asterisk (*) indicates the switch on which the command was entered.

Related Commands

show vcs

show fabric ecmp group

Displays the ECMP group information for the fabric RBridge IDs.

Syntax

show fabric ecmp group [**dest-rbridge** *number* | **src-rbridge** *number*]

Parameters

dest-rbridge *number*
Restricts the display output to the designated destination RBridge ID.

src-rbridge *number*
Restricts the display output to the designated source RBridge ID.

Modes

Privileged EXEC mode

Examples

Typical command output for the **show fabric ecmp group** command.

```
switch# show fabric ecmp group

Source RBridge-Id: 1
Total Path Count: 1

ECMP  Dst    Out    Out            Nbr   Nbr
Grp   RB-ID  Index  Interface      Index Interface      Hops BW    Trunk
------------------------------------------------------------------------
1     2      17     Te 1/8/18      25    Te 22/0/18     2    20G   Yes

        Source
        Range
        ------------
        1/8/1-48
        1/6/1-12

Source RBridge-Id: 1
Total Path Count: 1

ECMP  Dst    Out    Out            Nbr   Nbr
Grp   RB-ID  Index  Interface      Index Interface      Hops BW    Trunk
------------------------------------------------------------------------
1     3      17     Te 1/8/18      25    Te 22/0/18     3    20G   Yes

        Source
        Range
        ------------
        1/8/1-48
        1/6/1-12

Source RBridge-Id: 1
Total Path Count: 1

ECMP  Dst    Out    Out            Nbr   Nbr
Grp   RB-ID  Index  Interface      Index Interface      Hops BW    Trunk
------------------------------------------------------------------------
1     22     17     Te 1/8/18      25    Te 22/0/18     1    20G   Yes

        Source
        Range
        ------------
        1/8/1-48
        1/6/1-12

Source RBridge-Id: 1
Total Path Count: 1

ECMP  Dst    Out    Out            Nbr   Nbr
Grp   RB-ID  Index  Interface      Index Interface      Hops BW    Trunk
------------------------------------------------------------------------
1     160    17     Te 1/8/18      25    Te 22/0/18     2    20G   Yes

        Source
        Range
        ------------
        1/8/1-48
        1/6/1-12
```

History

Release version	Command history
5.0.0	This command was introduced.

show fabric ecmp load-balance

Displays the current configuration of hash field selection and hash swap.

Syntax

show fabric ecmp load-balance [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples

Some typical outputs of this command:

```
switch# show fabric ecmp load-balance

Fabric Ecmp Load Balance Information
------------------------------------
Rbridge-Id                  : 2
Ecmp-Load-Balance Flavor    : Destination MAC address and VID based load balancing
Ecmp-Load-Balance HashSwap  : 0x4
switch# show fabric ecmp load-balance rbridge-id 2

Fabric Ecmp Load Balance Information
------------------------------------
Rbridge-Id                  : 2
Ecmp-Load-Balance Flavor    : Destination MAC address and VID based load balancing
Ecmp-Load-Balance HashSwap  : 0x4
```

Related Commands

show fabric isl, show fabric trunk

show fabric isl

Displays Inter-Switch Link (ISL) information in the fabric.

Syntax

show fabric isl [*rbridge-id* | **all**]

Parameters

rbridge-id

Specifies an RBridge ID.

all

Specifies all switches in the fabric.

Modes

Privileged EXEC mode

Command Output

The **show fabric isl** command displays the following information:

Output field	Description
Rbridge-id	RBridge-id of the switch. Valid values range from 1 through 239.
#ISLs	Number of ISLs connected.
Src Index	Source index of the local RBridge.
Src Interface	Source interface of the local RBridge in the format "local-rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	Neighbor Index of the ISL connected from local port. If the link is segmented and the NBR rbridge details are unavailable, "?" displays in this field.
Nbr Interface	Neighbor interface of the ISL connected from the local RBridge in the format "nbr-rbridgeid/slot/port". If the ISL is not completely up, this field will be displayed as "?/?/?".
Nbr-WWN	Neighbor WWN of the switch. If the ISL is segmented and the neighbor RBridge details are not available, then "??:??:??:??:??:??:??:??" displays in this field.
BW	Bandwidth of the traffic.
Trunk	Displays "Yes" if trunk is enabled in the ISL.
Nbr-Name	Neighbor switch name.

Examples

This example displays Inter-Switch Link (ISL) information in the fabric.

```
switch# show fabric isl

Rbridge-id: 76 #ISLs: 2
Src       Src         Nbr       Nbr
 Index    Interface     Index    Interface             Nbr-WWN           BW   Trunk  Nbr-Name
------------------------------------------------------------------------------------------
 2     Te 1/0/2        56     Te 21/0/56     10:00:00:05:33:13:5F:BE  60G   Yes   "Edget12r1_1_21"
 7     Te 1/0/7        55     Te 22/0/55     10:00:00:05:33:40:31:93  40G   Yes   "Edget12r12_22"
```

This example displays ISL information and includes a segmented link.

```
switch# show fabric isl

Rbridge-id: 2 #ISLs: 4
Src       Src        Nbr        Nbr
Index    Interface    Index    Interface         Nbr-WWN              BW   Trunk   Nbr-Name
-------------------------------------------------------------------------------------
1       Te 2/0/1      1       Te 3/0/1      10:00:00:05:1E:CD:7A:7A  10G   Yes    "sw0"
2       Te 2/0/2      ?       Te ?/?/?      ??:??:??:??:??:??:??:?? (segmented - incompatible)
26      Te 2/0/26     56      Te 25/0/56    10:00:00:05:33:40:2F:C9  60G   Yes    "Edget12r31_25"
34      Te 2/0/34     58      Te 26/0/58    10:00:00:05:33:41:1E:B7  40G   Yes    "Edget12r32_26"
```

This example displays ISL information and includes an Fi port.

```
switch# show fabric isl

Rbridge-id: 66 #ISLs: 5
 Src         Src         Nbr       Nbr
Index     Interface     Index    Interface      Nbr-WWN                   BW   Trunk  Nbr-Name
-------------------------------------------------------------------------------------------
  5       Te 66/0/5      1       Te 65/0/1     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 15       Te 66/0/15     2       Te 65/0/2     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 25       Te 66/0/25     3       Te 65/0/3     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
 35       Te 66/0/35     4       Te 65/0/4     10:00:00:05:33:5F:EA:A4   10G   Yes   "sw0"
124       Fi 66/0/4      7       Fi 2/-/-      50:00:51:E4:44:40:0E:04   32G   Yes   "fcr_fd_2"
```

This ISL output example includes breakout information for switches on which breakout mode is configured.

```
switch# show fabric isl
Rbridge-id: 66 #ISLs: 5
Src Src Nbr Nbr
Index Interface Index Interface     Nbr-WWN                 BW Trunk Nbr-Name
-------------------------------------------------------------------------------------------
5   Te 66/0/5:1  1    Te 65/0/1    10:00:00:05:33:5F:EA:A4 10G Yes "sw0"
15  Te 66/0/15   2    Te 65/0/2:1  10:00:00:05:33:5F:EA:A4 10G Yes "sw0"
25  Te 66/0/25   3    Te 65/0/3    10:00:00:05:33:5F:EA:A4 10G Yes "sw0"
35  Te 66/0/35:1 4    Te 65/0/4:4  10:00:00:05:33:5F:EA:A4 10G Yes "sw0"
124 Fi 66/0/4    7    Fi 2/-/-     50:00:51:E4:44:40:0E:04 32G Yes "fcr_fd_2"
```

This example displays ISL details and includes the breakout index of the interface (for a non-trunked port) in normal mode.

```
switch# sh fab isl
Rbridge-id: 1   #ISLs: 4
 Src         Src        Nbr        Nbr
Index     Interface     Index    Interface      Nbr-WWN                   BW   Trunk  Nbr-Name
-------------------------------------------------------------------------------------
30        Te 1/0/27      1       Te 48/0/49:1   XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
32        Te 1/0/29      2       Te 48/0/49:2   XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
34        Te 1/0/31      3       Te 48/0/49:3   XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
36        Te 1/0/33      4       Te 48/0/49:4   XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
```

This example displays ISL details and includes the breakout index of the interface (for a trunked port) in normal mode.

```
switch# sh fab isl
Rbridge-id: 1   #ISLs: 1
 Src          Src         Nbr     Nbr
Index     Interface     Index   Interface          Nbr-WWN                    BW   Trunk  Nbr-Name
------------------------------------------------------------------------------
 5     Te 1/0/50:1       1       Te 48/0/49:1    10:00:00:05:33:E5:C1:8F   40G   Yes   "sw0"
```

This example displays ISL details in mixed mode, but no breakout index is displayed for switches running Network OS versions earlier than v4.1.0.

Output shown is for Network OS 4.0.0 for a non-trunked port in mixed mode.

```
sw0# sh fab isl
Rbridge-id: 1   #ISLs: 4
 Src       Src           Nbr       Nbr
Index   Interface       Index   Interface              Nbr-WWN           BW   Trunk  Nbr-Name
------------------------------------------------------------------------------------------
30      Te 1/0/27        1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
32      Te 1/0/29        1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
34      Te 1/0/31        1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
36      Te 1/0/33        1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
```

Output shown is for Network OS 4.0.0 for a trunked port in mixed mode.

```
sw0# sh fab isl
Rbridge-id: 1   #ISLs: 1
 Src       Src           Nbr       Nbr
Index   Interface       Index   Interface              Nbr-WWN           BW   Trunk  Nbr-Name
------------------------------------------------------------------------------------------
2      Te 1/0/50       1      Te 48/0/49      10:00:00:05:33:E5:C1:8F     40G   Yes   "sw0"
```

Output shown is for Network OS 4.1.0 for a non-trunked port in mixed mode.

```
sw0# sh fab isl
Rbridge-id: 48   #ISLs: 4
 Src       Src           Nbr       Nbr
Index   Interface       Index   Interface              Nbr-WWN            BW   Trunk  Nbr-Name
-------------------------------------------------------------------------------------------
1      Te 48/0/49:1       30      Te 1/0/25      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
1      Te 48/0/49:2       32      Te 1/0/27      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
1      Te 48/0/49:3       34      Te 1/0/29      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
1      Te 48/0/49:4       36      Te 1/0/31      XX:XX:XX:XX:XX:XX:XX:XX   10G   Yes   "sw0"
```

Output shown is for Network OS 4.1.0 for a trunked port in mixed mode.

```
sw0# sh fab isl
Rbridge-id: 1   #ISLs: 1
 Src       Src           Nbr       Nbr
Index   Interface       Index   Interface              Nbr-WWN            BW   Trunk  Nbr-Name
-------------------------------------------------------------------------------------------
30      Te 1/0/50:1       1      Te 48/0/49      10:00:00:05:33:E5:C1:8F   40G   Yes   "sw0"
```

Related Commands

fabric isl enable, show diag burninstatus, show fabric isl, show fabric trunk

show fabric islports

Displays information for all Inter-Switch Link (ISL) ports in the switch.

Syntax

show fabric islports [**rbridge-id** *rbridge-id*] [**all**]

Parameters

rbridge-id *rbridge-id*

Specifies the RBridge ID on which the ISL ports are displayed.

all

Specifies that information for all RBridges in the fabric are displayed.

Modes

Privileged EXEC mode

Usage Guidelines

If this command is executed without operands, it displays the ISL information of the local RBridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Command Output

The **show fabric islports** command displays the following information:

Output field	Description
Name	Switch name.
Type	Switch model and revision number.
State	Switch state. The valid values are Online, Offline, Testing, or Faulty.
Role	Switch role. The valid values are Principal, Subordinate, or Disabled.
VCS	Id VCS ID. Valid values range from 1 through 8192.
Config Mode	Brocade VCS Fabric mode. The valid values are Standalone/Local-Only/Distributed.
Rbridge-id	RBridge ID of the switch. Valid values range from 1 through 239.
WWN	Switch world wide name (WWN).
FCF MAC	Mac address
Index	A number between 0 and the maximum number of supported ports on the platform. The port index identifies the port number relative to the switch.
Interface	Interface of the local RBridge in the format “local-rbridge-id/slot/port”.

Output field	Description
State	Port state information: • Up—if the ISL is connected and the link is up. • Down—no ISL is connected.
Operational State	ISL state information: • ISL Fabric port—displays the world wide name (WWN) and name of the attached switch. • (Trunk Primary) —the port is the master port in a group of trunking ports. • (Trunk port, primary is rbridge-id/slot/port) —the port is configured as a trunking port; the primary port is rbridge-id/slot/port. • (upstream)—the ISL is an upstream path toward the principal switch of the fabric. • (downstream)—the ISL is a downstream path away from the principal switch of the fabric. • Segmented, (Reason Code)—the ISL has been segmented due to the given reason code. • Down, (Reason Code)—the ISL is down due to the given reason code.

In this command, ISL segmentation is denoted as "ISL segmented, (segmentation reason)". The segmentation reason could be any of those listed below.

TABLE 15 Segmentation reasons

Number	Segmentation	Explanation
1	RBridge ID Overlap	When a new node joins the cluster with the RBridge-id already existing in the cluster.
2	ESC mismatch, Unknown	Only on one side of the ISL, the actual ESC mismatch reason code will be displayed. On the other end, Unknown will be displayed.
3	ESC mismatch, Config Mode	Brocade VCS Fabric mode is different on both switches.
4	ESC mismatch, Distributed Config DB	The DCM Configuration DB is different on both the ends of ISL.
5	ESC mismatch, Brocade VCS Fabric License	Brocade VCS Fabric license is enabled on one end and disabled on the other side.
6	ESC mismatch, Fabric Distribution Service	FDS state is different on both the ends.
7	zone conflict	Zone configuration is not same on both the switches.
8	ISL Disabled	This port is disabled to be an ISL.
9	ISL Isolated	If BF or DIA is rejected then the port will get isolated.
10	LD inc om pat ability	ECP rejected or retries exceeded.
11	FDS Zone Conflict	FDS configuration caused zone conflict.
12	ESC mismatch, VCS Virtual Fabric Mode Conflict	Virtual Fabric mode is enabled on one end and disabled on the other end.

In this command, disabled ports are denoted as "Down (Disabled reason)". The disabled reason could be any of those listed below.

TABLE 16 Disabled port reasons

Number	Disabled Reasons	Explanation
1	Admin	Port is persistently disabled.
2	Protocol Incomplete	The ISL couldn't complete the link protocol. Stuck in G_PORT state.
3	RBridge ID Overlap	Two nodes in the cluster requested for same RBridge ID.
4	Long distance inc om pat ability	Long distance configuration doesn't match.
5	ELP retries exceeded	Max ELP retires exceeded but no response from the other end.
6	Zone conflict	Zoning configuration overlaps.
7	ESC Config Mode Conflict	The link has been segmented due to different Brocade VCS Fabric mode.
8	ESC NOS incompatible	Other end does not support Brocade VCS Fabric technology.
9	ESC Distributed Config DB Conflict	DCM Configuration DB conflict.
10	ESC VCS Fabric License Conflict	Brocade VCS Fabric license is not enabled on one end.
11	No VCS Fabric License	Brocade VCS Fabric license is not enabled. For more than 2 nodes in the cluster VCS fabric license is mandatory.
12	ESC Fabric Distribution Service Conflict	FDS state is different.
13	Zoning FDS Configuration Conflict	FDS zoning configuration is different.

Examples

To display information for all ISL ports in the core switch:

```
switch# show fabric islports
Name:       sw0
Type:       96.5
State:      Online
Role:       Fabric Principal
VCS Id:     1
Config Mode:Local-Only
Rbridge-id: 23
WWN:        10:00:00:05:33:d1:3a:ac
FCF MAC:    00:05:33:d1:3a:ac
Index   Interface      State   Operational State
=====================================================================
  0     Fi 23/0/1         Up    ISL (protocol incomplete)
  1     Fi 23/0/2         Up    F-Port
  2     Fi 23/0/3         Up    F-Port
  3     Fi 23/0/4         Up    F-Port
  4     Fi 23/0/5         Up    Loopback-> Fi 23/0/5
  5     Fi 23/0/6         Down
  6     Fi 23/0/7         Down
  7     Fi 23/0/8         Down
  8     Te 23/0/1         Up    ISL segmented,(ESC mismatch, Config Mode)(Trunk Primary)
  9     Te 23/0/2         Down
 10     Te 23/0/3         Down
 11     Te 23/0/4         Down
 12     Te 23/0/5         Down
 13     Te 23/0/6         Down
 14     Te 23/0/7         Down
 15     Te 23/0/8         Down
 16     Te 23/0/9         Down
 17     Te 23/0/10        Down
 18     Te 23/0/11        Down
 19     Te 23/0/12        Down
 20     Te 23/0/13        Down
 21     Te 23/0/14        Down
 22     Te 23/0/15        Down
 23     Te 23/0/16        Down
 24     Te 23/0/17        Down
 25     Te 23/0/18        Down
 26     Te 23/0/19        Down
 27     Te 23/0/20        Down
 28     Te 23/0/21        Down
 29     Te 23/0/22        Down
 30     Te 23/0/23        Down
 31     Te 23/0/24        Down
```

Related Commands

fabric isl enable, show diag burninstatus, show fabric isl, show fabric trunk

show fabric port-channel

Displays the fabric VLAG load-balance information.

Syntax

show fabric port-channel [*port-channel-id* | **load-balance**]

Parameters

port-channel-id
: Displays the information for the port channel ID.

load-balance
: Displays the load balance information.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples

```
switch# show fabric port-channel 10 load-balance
Fabric Vlag Load-Balance Information
------------------------------
Port-channel id     : 10
Load-Balance Flavor : Source and Destination MAC address and VID based load balancing
```

Related Commands

show fabric isl, show fabric trunk

show fabric route linkinfo

Displays the RBridge route link information connected in the fabric.

Syntax

show fabric route linkinfo

Modes

Privileged EXEC mode

Usage Guidelines

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

The output displays the link information, which includes the breakout index of the interface if breakout mode is configured in the source or neighbor interface.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0.

Command Output

The **show fabric route linkinfo** command displays the following information:

Output field	Description
Rbridge-id	ID of the RBridge. Valid values range from 1 through 239.
Reachable	Indicates whether the RBridge can be reached. Displays "Yes" if it is reachable, otherwise displays "No".
Version	Displays the version.
No. of links	The number of ISLs connected to the neighbor switches.
Link #	A sequence number for links on the RBridge.
Src Index	E_Port interface on the local switch. This value is typically equal to the Index field reported in the switchShow command.
Src Interface	Source interface of the local RBridge in the format "local-rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	E_Port interface on the remote switch. This value is typically equal to the index field reported in the switchShow command. If the link is segmented and the NBR rbridge details are unavailable, "?" displays in this field.
Nbr Interface	Neighbor interface of the ISL connected from the local RBridge in the format "nbr-rbridgeid/slot/port". If the ISL is not completely up, this field will be displayed as "?/?/?".
Link-Cost	The cost of reaching the destination domain.
Link-type	The type of link.
Trunk	Displays "Yes" if trunk is enabled in the ISL, otherwise displays "No".

Examples

To display link information for the fabric:

```
switch# show fabric route linkinfo

Rbridge-id: 1
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       1        Fi 1/-/-      128      Fi 2/-/-       10000       Pt_Pt
2       159      Fi 1/-/-      128      Fi 160/-/-     10000       Pt_Pt
Rbridge-id: 2
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       129      Fi 2/-/-      49       Fi 66/0/1      10000       Pt_Pt
2       128      Fi 2/-/-      1        Fi 1/-/-       10000       Pt_Pt
Rbridge-id: 65
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       2        Te 65/0/2     2        Te 66/0/2      500         Pt_Pt Ethernet   Yes
2       44       Te 65/0/44    20       Te 66/0/20     500         Pt_Pt Ethernet   Yes
Rbridge-id: 66
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       2        Te 66/0/2     2        Te 65/0/2      500         Pt_Pt Ethernet   Yes
2       20       Te 66/0/20    44       Te 65/0/44     500         Pt_Pt Ethernet   Yes
3       49       Fi 66/0/1     129      Fi 2/-/-       500         Pt_Pt            Yes
4       54       Fi 66/0/6     129      Fi 160/-/-     500         Pt_Pt            Yes
Rbridge-id: 160
===============
Reachable:    Yes
Version:      1
No. of Links: 2
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index    Interface      Link-Cost   Link-Type        Trunk
-------------------------------------------------------------------------------------------
1       129      Fi 160/-/-    54       Fi 66/0/6      10000       Pt_Pt
2       128      Fi 160/-/-    159      Fi 1/-/-       10000       Pt_Pt
```

This example displays link linformation and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route linkinfo
Rbridge-id: 1
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src          Nbr        Nbr
        Index     Interface     Index     Interface     Link-Cost    Link-Type         Trunk
-------------------------------------------------------------------------------------------
1       28       Te 1/0/49:1     0      Te 48/0/49:1    500          Pt_Pt Ethernet
2       30       Te 1/0/49:2     1      Te 48/0/49:2    500          Pt_Pt Ethernet
3       32       Te 1/0/49:3     2      Te 48/0/49:3    500          Pt_Pt Ethernet
4       34       Te 1/0/49:4     3      Te 48/0/49:4    500          Pt_Pt Ethernet
Rbridge-id: 48
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src          Nbr        Nbr
        Index     Interface     Index     Interface     Link-Cost    Link-Type         Trunk
-------------------------------------------------------------------------------------------
1       0        Te 48/0/49:1    28     Te 1/0/49:1     500          Pt_Pt Ethernet
2       1        Te 48/0/49:2    30     Te 1/0/49:2     500          Pt_Pt Ethernet
3       2        Te 48/0/49:3    32     Te 1/0/49:3     500          Pt_Pt Ethernet
4       3        Te 48/0/49:4    34     Te 1/0/49:4     500          Pt_Pt Ethernet
```

This example displays link linformation and includes the breakout index of the interface in mixed mode running Network OS v4.0.0:

```
switch# show fabric route linkinfo
Rbridge-id: 1
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src          Nbr        Nbr
        Index    Interface     Index     Interface   Link-Cost      Link-Type         Trunk
-------------------------------------------------------------------------------------------
1       28       Te 1/0/49     0      Te 48/0/49       500          Pt_Pt Ethernet
2       30       Te 1/0/49     1      Te 48/0/49       500          Pt_Pt Ethernet
3       32       Te 1/0/49     2      Te 48/0/49       500          Pt_Pt Ethernet
4       34       Te 1/0/49     3      Te 48/0/49       500          Pt_Pt Ethernet
Rbridge-id: 48
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src          Nbr        Nbr
        Index    Interface     Index     Interface   Link-Cost     Link-Type         Trunk
-------------------------------------------------------------------------------------------
1       0        Te 48/0/49    28     Te 1/0/49        500          Pt_Pt Ethernet
2       1        Te 48/0/49    30     Te 1/0/49        500          Pt_Pt Ethernet
3       2        Te 48/0/49    32     Te 1/0/49        500          Pt_Pt Ethernet
4       3        Te 48/0/49    34     Te 1/0/49        500          Pt_Pt Ethernet
```

This example displays link linformation and includes the breakout index of the interface in mixed mode running Network OS v4.1.0:

```
switch# show fabric route linkinfo
Rbridge-id: 1
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index     Interface      Link-Cost     Link-Type       Trunk
-------------------------------------------------------------------------------------------
1       28       Te 1/0/49:1     0      Te 48/0/49         500         Pt_Pt Ethernet
2       30       Te 1/0/49:2     1      Te 48/0/49         500         Pt_Pt Ethernet
3       32       Te 1/0/49:3     2      Te 48/0/49         500         Pt_Pt Ethernet
4       34       Te 1/0/49:4     3      Te 48/0/49         500         Pt_Pt Ethernet
Rbridge-id: 48
===============
Reachable:    Yes
Version:      1
No. of Links: 4
Link#    Src        Src         Nbr        Nbr
        Index    Interface     Index     Interface      Link-Cost     Link-Type       Trunk
-------------------------------------------------------------------------------------------
1       0        Te 48/0/49:1    28     Te 1/0/49          500         Pt_Pt Ethernet
2       1        Te 48/0/49:2    30     Te 1/0/49          500         Pt_Pt Ethernet
3       2        Te 48/0/49:3    32     Te 1/0/49          500         Pt_Pt Ethernet
4       3        Te 48/0/49:4    34     Te 1/0/49          500         Pt_Pt Ethernet
```

Related Commands

show fabric route topology, show fabric route neighbor-state

show fabric route multicast

Displays ISLs that receives any forwarded Broadcast, unknown Unicast, and Multicast (BUM) traffic.

Syntax

show fabric route multicast [*rbridge-id* | **all**]

Parameters

rbridge-id

Specifies an RBridge ID.

all

Specifies all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

The multicast routing information indicates all ports that are members of the multicast distribution tree ports that are able to send and receive multicast frames.

If this command is executed without operands, it displays the multicast information of the local RBridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0. In such instances, the neighbor port WWN (Nbr-WWN) is displayed as *XX:XX:XX:XX:XX:XX:XX:XX* .

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Command Output

The **show fabric route multicast** command displays the following information:

Output field	Description
Rbridge-id	RBridge ID of the switch. Valid values range from 1 through 239.
Mcast Priority	Mcast priority value of the switch. Valid values range from 1 through 255.
Enet IP Addr	The switch Ethernet IP address.
WWN	World Wide Name of the switch.
Name	Switch name.
Src-Index	Source index of the local RBridge.

Output field	Description
Src-Port	Source port of the local RBridge in the format “local-rbridge-id/slot/port”.
Nbr-Index	Neighbor Index of the ISL connected from local port.
Nbr-Port	Neighbor port of the ISL connected from the local RBridge in the format “nbr-rbridge-id/slot/port”.

Examples

To display the multicast routing information for all ports in the switch:

```
switch# show fabric route multicast

Root of the Multicast-Tree
==========================
Rbridge-id: 1
Mcast Priority: 1
Enet IP Addr: 10.24.85.212
WWN: 10:00:00:05:1e:cd:73:fa
Name: switch
Rbridge-id: 1
Src-Index    Src-Port     Nbr-Index    Nbr-Port    BW      Trunk
-----------------------------------------------------------------
7            Te 1/0/7         55      Te 22/0/55   40G      Yes
15           Te 1/0/15        57      Te 23/0/57   60G      Yes
22           Te 1/0/22        58      Te 24/0/58   40G      Yes
26           Te 1/0/26        56      Te 25/0/56   60G      Yes
34           Te 1/0/34        58      Te 26/0/58   60G      Yes
41           Te 1/0/41        59      Te 27/0/59   20G      Yes
44           Te 1/0/44        56      Te 28/0/56   60G      Yes
```

This example displays route information and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route multicast
Root of the Multicast-Tree
==========================
 Rbridge-id: 1
 Mcast Priority: 1
 Enet IP Addr: 10.38.19.47
 WWN: 10:00:00:05:33:65:0b:20
 Name: sw0
Rbridge-id: 48
Src-Index   Src-Port       Nbr-Index   Nbr-Port        BW   Trunk
-----------------------------------------------------------------
0         Te 48/0/49:1       28       Te 1/0/49:1      0G
```

This example displays route information and includes the breakout index of the interface in mixed mode running Network OS v4.0.0.

```
sw0# show fabric route multicast
Root of the Multicast-Tree
==========================
 Rbridge-id: 1
 Mcast Priority: 1
 Enet IP Addr: 10.38.19.47
 WWN: 10:00:00:05:33:65:0b:20
 Name: sw0
Rbridge-id: 1
Src-Index   Src-Port      Nbr-Index   Nbr-Port        BW    Trunk
-----------------------------------------------------------------
28         Te 1/0/49         0       Te 48/0/49       10G
```

This example displays route information and includes the breakout index of the interface in mixed mode running Network OS v4.1.0.

```
sw0# show fabric route multicast
Root of the Multicast-Tree
==========================
 Rbridge-id: 1
 Mcast Priority: 1
 Enet IP Addr: 10.38.19.47
 WWN: 10:00:00:05:33:65:0b:20
 Name: sw0
Rbridge-id: 1
Src-Index   Src-Por        Nbr-Index   Nbr-Port        BW    Trunk
-------------------------------------------------------------------
0         Te 48/0/49:1        28       Te 1/0/49       10G
```

Related Commands

fabric route mcast, show fabric route topology, show running-config fabric route mcast, show fabric route topology

show fabric route neighbor-state

Displays the state information of all the ISL links connected to the RBridge.

Syntax

show fabric route neighbor-state [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

FSPF defines a neighbor as a remote ISL interface that is directly attached to the local RBridge. If the interfaces are trunked, the command displays data only about the trunk primary.

If no information is available for the switch, the command displays the message "No ISL found."

If no RBridge is specified, the neighbor state information for the local switch is displayed.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0.This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Command Output

The **show fabric route neighbor-state** command displays the following information:

Output field	Description
rbridge-id	ID of the RBridge. Valid values range from 1 through 239.
# ISLs	The number of ISLs that connect the switch to neighbor switches.
Src Index	E_Port interface on the local switch. This value is typically equal to the Index field reported in the switchShow command.

Output field	Description
Src Interface	Physical interface on the local switch in the format "Te rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	E_Port interface on the remote switch. This value is typically equal to the index field reported in the switchShow command.
Nbr Interface	Physical interface on the remote switch in the format "Te rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr State	The FSPF neighbor state for the port attached to remote switch. The neighbor can be in one of the following states: • NB_ST_DOWN—the neighbor is down. • NB_ST_INIT—the neighbor is initializing. • NB_ST_DB_EX—the neighbor and the switch are exchanging data from their Link State Records (LSR) databases. • NB_ST_DB_ACK_WT—the neighbor is waiting for the switch to acknowledge the LSR database. • NB_ST_DB_WT—the LSR Database is in waiting state; synchronization is in process. • NB_ST_FULL—the neighbor is in the last, finishing state. The E_Port can route frames only if the neighbor is in full state.

Examples

To display the state of FSPF neighbors for the local switch:

```
switch# show fabric route neighbor-state

Rbridge-id: 66   #ISLs: 8
 Src     Src              Nbr      Nbr            Nbr
Index   Interface        Index  Interface        State
-----------------------------------------------------
2       Te 66/0/2        2      Te 65/0/2       NB_ST_FULL
17      Te 66/0/17       41     Te 65/0/41      NB_ST_FULL
18      Te 66/0/18       42     Te 65/0/42      NB_ST_FULL
19      Te 66/0/19       43     Te 65/0/43      NB_ST_FULL
20      Te 66/0/20       44     Te 65/0/44      NB_ST_FULL
23      Te 66/0/23       47     Te 65/0/47      NB_ST_FULL
49      Fi 66/0/1        129    Fi 2/-/-        NB_ST_FULL
53      Fi 66/0/5        129    Fi 160/-/-      NB_ST_FULL
```

This example displays neighbor state route details and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route neighbor-state
Rbridge-id: 1   #ISLs: 1
Src     Src              Nbr      Nbr            Nbr
Index   Interface        Index  Interface        State
-----------------------------------------------------
30      Te 1/0/49:1       1     Te 48/0/49:1     NB_ST_FULL
```

This example displays neighbor state route details of the non-trunked port in mixed mode running Network OS v4.0.0. (In mixed mode, the QSFP breakout index is not displayed in the output on a switch running Network OS versions earlier than v4.1.0.)

```
sw0# show fabric route neighbor-state
Rbridge-id: 1   #ISLs: 2
Src     Src              Nbr      Nbr            Nbr
Index   Interface        Index  Interface        State
-----------------------------------------------------
30      Te 1/0/49        1      Te 48/0/49       NB_ST_FULL
```

This example displays neighbor state route details of the non-trunked port in mixed mode running Network OS v4.1.0.

```
sw0# show fabric route neighbor-state
Rbridge-id: 1   #ISLs: 2
Src     Src             Nbr      Nbr            Nbr
Index   Interface       Index  Interface        State
-----------------------------------------------------------
30      Te 1/0/49:1     1      Te 48/0/49       NB_ST_FULL
```

Related Commands

show fabric route topology, show fabric route linkinfo

show fabric route pathinfo

Displays the path of a data stream through a fabric and provides statistics about each hop on that path.

Syntax

show fabric route pathinfo Fabric ID Domain Source Port Destination Port Basic Stats Extended Stats Reverse Path

Parameters

You are prompted to select parameters interactively. The command will prompt you for the following parameters:

Fabric ID

Enter the VCS ID of the destination Network OS switch or the Fabric ID of the destination Fabric OS switch. If unspecified, the value defaults to –1, which specifies the Brocade VCS Fabric cluster of the local switch.

Domain

Enter the RBridge ID of the destination Network OS switch or the domain ID of the destination Fabric OS switch. You must enter a value for this parameter. It has no default value.

Source Port

Enter the port index of the port at the head of the data stream to be traced. traced. If unspecified, the value defaults to –1, which specifies the embedded port.

Destination Port

Enter the port index of the port on the destination switch for the path being traced. If unspecified, the value defaults to –1, which specifies the embedded port. The command output also reports the status of the Destination Port. If the specified port is out of range on the destination switch, the command fails with the message "Target port not present."

Basic Stats

Enter **y** to display basic statistics about each hop. By default, basis statistics are not displayed.

Extended Stats

Enter **y** to display extended statistics about each hop. By default, extended statistics are not displayed.

Reverse Path

Enter **y** to display reverse path information in addition to the forward path information. By default, reverse path information is not displayed.The path from port A on switch X to port B on switch Y might be different from the path from port B to port A depending on the links traversed between a given sequence of switches, or the reverse path might involve different switches.

Modes

Privileged EXEC mode

Usage Guidelines

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Use this command to display detailed routing information and statistics for a data stream from a source port on the local switch to a destination port on another switch. The destination switch can be a member of the same Brocade VCS Fabric cluster, a member of a different Brocade VCS Fabric cluster, a member of a Fabric OS backbone fabric, or a member of a Fabric OS edge fabric. This routing information describes the exact path that a user data stream takes to go from the source port to the destination port.

Use this command to check whether a congested link might be causing performance degradation on a specific data stream or path.

You can request statistics for each hop in addition to the routing information. These statistics are presented for the input and output ports for both receive and transmit modes. You can select basic statistics, extended statistics, or both. Statistics are not reported for the embedded port. Some throughput values are reported in multiple time intervals to describe current path utilization and the average throughput over a longer period of time.

To collect these statistics, this command uses a special frame that is sent hop-by-hop from the source switch to the destination switch. To prevent such a frame from looping forever if an error occurs, a maximum of 25 hops is enforced. The hop count includes all hops in the direct path from source to destination, and also all the hops in the reverse path, if the tracing of the reverse path is requested. If the hop limit is exceeded, information collected up to the switch that returned the error is displayed along with the message "Maximum hops exceeded."

Command Output

Regardless of parameter selection, the **show fabric route pathinfo** command displays the following information of the destination port and routing information about each hop:

Output field	Description
Target port is	Provides the status of the destination port. It can have one of the following values: • Embedded—this is the embedded port. • Not active—the port is not connected or is still initializing and has not yet reached a stable state. • E_Port • F_Port
Hop	The hop number. The local switch is hop 0.
In Port	The port index of the port that the frames come in from on this path. For hop 0, this is the source port.
Domain ID	Routing bridge ID of the Network OS switch or domain of the Fabric OS switch.
Out Port	The port index of the port that the frames use to reach the next hop on this path. For the last hop, this is the destination port.
BW	The bandwidth of the output ISL in Gbps. It does not apply to the embedded port.
Cost	The cost of the ISL used by the fabric shortest path first (FSPF) routing protocol. It applies only to an E_Port.

If basic statistics are requested, the following information is provided for each hop in addition to the routing information:

Output field	Description
B/s (1s)	Bytes per second transmitted and received over the previous 1-second period for the in port and for the out port.
B/s (64s)	Bytes per second transmitted and received over the previous 64-second period for the in port and for the out port.

Output field	Description
TxCrdz(1s)	The length of time, in milliseconds, over the previous 1 second interval that the port was unable to transmit frames because the transmit BB credit was 0. The purpose of this statistic is to detect congestion or a device affected by latency. This parameter is sampled at 1 millisecond (ms) intervals, and the counter is incremented if the condition is true. Each sample represents 1 ms of time with a 0 Tx BB Credit. An increment of this counter means that the frames could not be sent to the attached device for 1 ms, indicating degraded performance.
TxCrdz(64s)	The length of time, in milliseconds, over the previous 64-second interval that the port was unable to transmit frames because the transmit BB credit was 0.

If extended statistics are requested, the following information is provided for each hop in the data path:

Output field	Description
F/s (1s)	The number of frames received or transmitted per second over the previous 1-second period.
F/s (64s)	The number of frames received or transmitted per second over the previous 64-second period.
Words	The total number of 4-byte Fibre Channel words.
Frames	The total number of frames.
Errors	The total number of errors that may have caused a frame not to be received correctly. This includes cyclic redundancy check (CRC) errors, bad end-of-frame (EOF) errors, frame truncated errors, frame-too-short errors, and encoding errors inside a frame.

Examples

To show path information without statistics or reverse path information:

```
switch# show fabric route pathinfo

Fabric ID (1..128)[-1]    : 10

Domain    : 1

Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : n

Extended Stats [y/n/yes/no]?    : n

Reverse Path[y/n/yes/no]?    : n

------------------------------------------------------------------------
Target port is Embedded
Hop       In Port            Domain ID          Out Port    BW      Cost
------------------------------------------------------------------------
  0         E                   152               1        10G       500
  1         5                   142              54         4G       500
  2        14                     5               1         4G     10000
  3       217                   100             793        48G       500
  4      1209                     2             148         8G       500
  5         3                     1               E        --        --
```

To show path information with basic statistics:

```
switch# show fabric route pathinfo

Fabric ID (1..128)[-1]    : 10

Domain    : 1

Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : y

Extended Stats [y/n/yes/no]?    : n

Reverse Path[y/n/yes/no]?    : n

--------------------------------------------------------------------------
Target port is Embedded
Hop       In Port            Domain ID           Out Port    BW     Cost
--------------------------------------------------------------------------
  0         E                   152               1         10G      500
Port                      E                            1
                  ----------------------------------------------------
                        Tx              Rx              Tx              Rx
B/s (1s)                --              --               0               0
B/s (64s)               --              --               0               0
TxCrdz (1s)             --              --               0              --
TxCrdz (64s)            --              --               0              --
Hop       In Port            Domain ID           Out Port     BW     Cost
--------------------------------------------------------------------------
  1         5                   142               54           4G      500
Port                          5                            54
                        Tx              Rx              Tx              Rx
                        ----------------------------------------------------
B/s (1s)                 0               0               0               0
B/s (64s)                0               0               7               7
TxCrdz (1s)              0              --               0              --
TxCrdz (64s)             0              --               0              --
Hop       In Port            Domain ID           Out Port    BW     Cost
--------------------------------------------------------------------------
  2        14                   5               1          4G    10000
Port                          14                           1
                        Tx              Rx              Tx              Rx
                        ----------------------------------------------------
B/s (0s)                 0               0               0               0
B/s (0s)                 0               0               0               0
TxCrdz (0s)              0              --               0              --
TxCrdz (0s)              0              --               0              --
Hop       In Port            Domain ID           Out Port    BW     Cost
--------------------------------------------------------------------------
  3       217                 100               793        48G      500
Port                          217                          793
                        Tx              Rx              Tx              Rx
                        ----------------------------------------------------
B/s (1s)                 0               0               0               0
B/s (64s)                4               4               0               0
TxCrdz (1s)              0              --               0              --
TxCrdz (64s)             0              --               0              --
Hop       In Port            Domain ID           Out Port    BW     Cost
--------------------------------------------------------------------------
  4      1209                   2               148         8G      500
Port                        1209                           148
                        Tx              Rx              Tx              Rx
                        ----------------------------------------------------
B/s (1s)                 0               0               0               0
B/s (64s)                0               0               3               0
TxCrdz (1s)              0              --               0              --
TxCrdz (64s)             0              --               0              --
Hop       In Port            Domain ID           Out Port    BW     Cost
--------------------------------------------------------------------------
  5         3                   1                 E        --      --
```

```
Port                        3                       E
                          Tx              Rx              Tx              Rx
                          ------------------------------------------------
B/s (1s)                   0               0              --              --
B/s (64s)                  0               3              --              --
TxCrdz (1s)                0              --              --              --
TxCrdz (64s)               0              --              --              --
```

To show path information with extended statistics and reverse path information:

```
switch# show fabric route pathinfo

Fabric ID (1..128)[-1]    : 10

Domain    : 1

Source Port [-1]    :
Destination Port [-1]    :
Basic Stats [y/n/yes/no]?    : y

Extended Stats [y/n/yes/no]?    : y

Reverse Path[y/n/yes/no]?    : y

-----------------------------------------------------------------
Target port is Embedded
Hop       In Port            Domain ID           Out Port    BW     Cost
-------------------------------------------------------------------------
  0         E                   152                1        10G      500
Port                      E                                  1
                  Tx              Rx                 Tx              Rx
                  ------------------------------------------------------
B/s (1s)          --              --                  0               0
B/s (64s)         --              --                  0               0
TxCrdz (1s)       --              --                  0               --
TxCrdz (64s)      --              --                  0               --
F/s (1s)          --              --                  0               0
F/s (64s)         --              --                  0               0
Words             --              --                  0               0
Frames            --              --                  0               0
Errors            --              --                  --              0
Hop       In Port            Domain ID           Out Port    BW     Cost
-------------------------------------------------------------------------
  1        5                  142                54         4G      500
Port                          5                              54
                     Tx              Rx                 Tx              Rx
                     ------------------------------------------------------
B/s (1s)              0               0                  0               0
B/s (64s)             0               0                  7               7
TxCrdz (1s)           0               --                 0               --
TxCrdz (64s)          0               --                 0               --
F/s (1s)              0               0                  0               0
F/s (64s)             0               0                  0               0
words                 0               0                967             967
Frames                0               0               1204             967
Errors                --              0                  --              0
Hop       In Port            Domain ID           Out Port    BW     Cost
-------------------------------------------------------------------------
  2        14                  5                  1         4G    10000
Port                          14                       1
                     Tx              Rx                 Tx              Rx
                     ------------------------------------------------------
B/s (0s)              0               0                  0               0
B/s (0s)              0               0                  0               0
TxCrdz (0s)           0               --                 0               --
TxCrdz (0s)           0               --                 0               --
F/s (0s)              0               0                  0               0
F/s (0s)              0               0                  0               0
words
Frames
Errors                --              0                  --              0
Hop       In Port            Domain ID           Out Port    BW     Cost
-------------------------------------------------------------------------
  3       217                 100                793        48G      500
Port                          217                     793
                     Tx              Rx                 Tx              Rx
                     ------------------------------------------------------
B/s (1s)              0               0                  0               0
B/s (64s)             4               4                  0               0
```

```
TxCrdz (1s)            0              --              0              --
TxCrdz (64s)           0              --              0              --
F/s (1s)               0               0              0               0
F/s (64s)              0               0              0               0
words              50570           50570      511118479       511118479
Frames             50742           50570      539255694       511118479
Errors                --               0             --               0
Hop       In Port             Domain ID       Out Port      BW     Cost
------------------------------------------------------------------------
  4        1209                    2             148        8G      500
Port                          1209                    148
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0               0               0
B/s (64s)             0               0               3               0
TxCrdz (1s)           0              --               0              --
TxCrdz (64s)          0              --               0              --
F/s (1s)              0               0               0               0
F/s (64s)             0               0               0               0
words               608             608             424             424
Frames              454             608             563             424
Errors                --               0             --               0
Hop       In Port             Domain ID          Out Port    BW     Cost
------------------------------------------------------------------------
  5         3                     1                E         --       --
Port                          3                       E
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0              --              --
B/s (64s)             0               3              --              --
TxCrdz (1s)           0              --              --              --
TxCrdz (64s)          0              --              --              --
F/s (1s)              0               0              --              --
F/s (64s)             0               0              --              --
words              1244            1244              --              --
Frames              898            1244              --              --
Errors               --               0              --              --
       Reverse Path
Hop       In Port             Domain ID          Out Port    BW     Cost
------------------------------------------------------------------------
  6         E                     1                0          8G      500
Port                          E                       0
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              --              --              0               0
B/s (64s)             --              --              4               4
TxCrdz (1s)           --              --              0              --
TxCrdz (64s)          --              --              0              --
F/s (1s)              --              --              0               0
F/s (64s)             --              --              0               0
Words                 --              --            809             809
Frames                --              --           1645             809
Errors                --              --             --               0
Hop       In Port             Domain ID          Out Port    BW     Cost
------------------------------------------------------------------------
  7       149                     2               1204       48G      500
Port                          149                     1204
                     Tx              Rx              Tx              Rx
                     ------------------------------------------------
B/s (1s)              0               0               0               0
B/s (64s)             4               4               0               0
TxCrdz (1s)           0              --               0              --
TxCrdz (64s)          0              --               0              --
F/s (1s)              0               0               0               0
F/s (64s)             0               0               0               0
words               707             707              56              56
Frames              403             707              57              56
Errors                --               0             --               0
Hop       In Port             Domain ID          Out Port    BW     Cost
------------------------------------------------------------------------
  8        796                   100              217        4G      500
Port                          796                     217
```

```
                        Tx              Rx              Tx              Rx
                        ------------------------------------------------------
B/s (1s)                 0               0               0               0
B/s (64s)                0               0               4               4
TxCrdz (1s)              0              --               0              --
TxCrdz (64s)             0              --               0              --
F/s (1s)                 0               0               0               0
F/s (64s)                0               0               0               0
words             48267544        48267544           50570           50570
Frames             1164982        48267544           50742           50570
Errors                  --               0              --               0
```

Related Commands

show fabric route topology, show fabric route neighbor-state

show fabric route topology

Displays the RBridge routes from the source switch to destination switches.

Syntax

show fabric route topology [**src-rbridgeId** *src-id*] [**dst-rbridgeId** *dst_id*]

Parameters

src-rbridgeId

Specifies the source RBridge ID

src-id

Specifies details on the source RBridge.

dst-rbridgeId

Specifies the destination RBridge ID

dst_id

Specifies details on the destination RBridge.

Modes

Privileged EXEC mode

Usage Guidelines

The RBridge routes to other switches are the available paths to remote domains that unicast traffic can take.

The source RBridge ID must be the local RBridge ID in this release. It is an optional parameter. If you do not specify the source RBridge ID or the destination RBridge ID, the system routes to all destinations in the Fabric.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1. This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Command Output

The **show fabric route topology** command displays the following information:

Output field	Description
Path Count	The number of currently active paths to the destination domain.
Src RB-ID	RBridge ID of the source switch. Valid values range from 1 through 239.
Dst RB-ID	Destination rbridge-id to where the traffic flows. Valid values range from 1 through 255.

Output field	Description
Out Index	The port index to which incoming frames are forwarded to reach the destination RBridge.
Out Interface	The port interface (local-rbridge-id/slot/port) of the local RBridge to which incoming frames are forwarded to the destination RBridge. If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
ECMP Grp	The Equal Cost MultiPath group
Hops	The maximum number of hops to reach destination RBridge.
Cost	The cost of reaching destination domain.
Nbr Index	Neighbor Index of the ISL connected from local port.
Nbr Interface	Neighbor interface of the ISL connected from the local RBridge in the format "nbr-rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
BW	Bandwidth of the traffic.
Trunk	Displays "Yes" if trunk is enabled in the ISL.

Examples

To display the fabric route topology information:

```
switch# show fabric route topology
Total Path Count: 4

Src    Dst    Out    Out            ECMP            Nbr    Nbr
RB-ID  RB-ID  Index  Interface      Grp  Hops  Cost  Index  Interface      BW   Trunk
-------------------------------------------------------------------------------------
1      2      17     Te 1/8/18      1    2     1000  25     Te 22/0/18     20G   Yes
       3      17     Te 1/8/18      1    3     11000 25     Te 22/0/18     20G   Yes
       22     17     Te 1/8/18      1    1     500   25     Te 22/0/18     20G   Yes
       160    17     Te 1/8/18      1    2     1000  25     Te 22/0/18     20G   Yes
```

This example displays route topology details and includes the breakout index of the neighbor interface in normal mode.

```
switch# show fabric route topology
Total Path Count: 3
Src    Dst    Out    Out            ECMP            Nbr    Nbr
RB-ID  RB-ID  Index  Interface      Grp  Hops  Cost  Index  Interface      BW   Trunk
-------------------------------------------------------------------------------------
1      48     30     Te 1/0/49:1    1     1    500     1     Te 48/0/49:1  40G   Yes
```

This example displays route topology details and includes the breakout index of the neighbor interface in mixed mode running Network O.S. v4.0.0.

```
switch# show fabric route topology
Total Path Count: 3
Src    Dst    Out    Out            ECMP            Nbr    Nbr
RB-ID  RB-ID  Index  Interface      Grp  Hops  Cost  Index  Interface      BW   Trunk
-------------------------------------------------------------------------------------
  1      48     30    Te 1/0/49      1     1    500     1    Te 48/0/49    40G   Yes
```

This example displays route topology details and includes the breakout index of the neighbor interface in mixed mode running Network O.S. v4.1.0.

```
switch# show fabric route topology
Total Path Count: 3
Src    Dst    Out    Out            ECMP            Nbr    Nbr
RB-ID  RB-ID  Index  Interface      Grp  Hops  Cost  Index  Interface      BW   Trunk
-------------------------------------------------------------------------------------
  1      48     30    Te 1/0/49:1    1    1     500    1     Te 48/0/49     40G   Yes
```

Related Commands

fabric route mcast

show fabric trunk

Displays trunk information of Inter-Switch Link (ISL) ports.

Syntax

show fabric trunk [*rbridge-id* | **all**]

Parameters

rbridge-id

Specifies an RBridge ID.

all

Specifies all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

If this command is executed without operands, it displays the trunk information of the local RBridge.

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0. In such instances, the neighbor port WWN (Nbr-WWN) is displayed as *XX:XX:XX:XX:XX:XX:XX:XX* .

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Command Output

The **show fabric trunk** command displays the following information:

Output field	Description
Rbridge-id	RBridge ID of the switch. Valid values range from 1 through 239.
Trunk Group	Displays each trunking group on a switch. All ports that are part of this trunking group are displayed.
Src Index	Source index of the local RBridge.
Src Interface	Source interface of the local RBridge in the format "local-rbridge-id/slot/port". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr Index	Neighbor Index of the ISL connected from local port. If the link is segmented and the neighbor RBridge details are unavailable, "?" displays in this field.

Output field	Description
Nbr Interface	Neighbor interface of the ISL connected from the local RBridge in the format "nbr-rbridge-id/slot/port". If the ISL is not completely up, this field will be displayed as "?/?/?". If the ISL is not up, then "?/?/?" displays for a Te interface and "-/-/-" displays for an Fi interface.
Nbr-WWN	Neighbor WWN of the switch. If the ISL is segmented and the neighbor RBridge details are not available, then "??:??:??:??:??:??:??:??" displays in this field.

Examples

To display the fabric trunk information:

```
switch# show fabric trunk

Possible completions:
  all          all RBridges in fabric
  rbridge-id   Syntax: rbridge-id [rbridge-id]
  |            Output modifiers
  <cr>
switch# show fabric trunk

Rbridge-id: 65
Trunk  Src    Source          Nbr     Nbr
Group  Index  Interface       Index   Interface       Nbr-WWN
--------------------------------------------------------------------------------
1      1      Te 65/0/1       1       Te 66/0/1       10:00:00:05:33:6F:27:57
1      2      Te 65/0/2       2       Te 66/0/2       10:00:00:05:33:6F:27:57
2      45     Te 65/0/45      21      Te 66/0/21      10:00:00:05:33:6F:27:57
2      47     Te 65/0/47      23      Te 66/0/23      10:00:00:05:33:6F:27:57
2      46     Te 65/0/46      22      Te 66/0/22      10:00:00:05:33:6F:27:57
```

This example displays trunk details and includes the breakout index of the neighbor interface in normal mode.

```
sw0# show fabric trunk
Rbridge-id: 1
Trunk  Src    Source           Nbr      Nbr
Group  Index  Interface       Index    Interface         Nbr-WWN
--------------------------------------------------------------------------------
 1      74      Te 1/0/49:1     0      Te 48/0/49:1      XX:XX:XX:XX:XX:XX:XX:XX
 1      76      Te 1/0/49:2     1      Te 48/0/49:2      XX:XX:XX:XX:XX:XX:XX:XX
 1      80      Te 1/0/49:3     3      Te 48/0/49:3      XX:XX:XX:XX:XX:XX:XX:XX
 1      78      Te 1/0/49:4     2      Te 48/0/49:4      XX:XX:XX:XX:XX:XX:XX:XX
Where XX:XX:XX:XX:XX:XX:XX:XX is the neighbor port WWN
```

This example displays trunk details and includes the breakout index of the neighbor interface in mixed mode running Network OS v4.0.0.

```
sw0# show fabric trunk
Rbridge-id: 1
Trunk  Src     Source           Nbr      Nbr
Group  Index   Interface       Index    Interface         Nbr-WWN
--------------------------------------------------------------------------------
 1      74      Te 1/0/49        0      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      76      Te 1/0/49        1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      80      Te 1/0/49        3      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      78      Te 1/0/49        2      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
```

This example displays trunk details and includes the breakout index of the neighbor interface in mixed mode running Network OS v4.1.0.

```
sw0# show fabric trunk
Rbridge-id: 1
Trunk  Src     Source           Nbr      Nbr
Group  Index   Interface       Index    Interface        Nbr-WWN
------------------------------------------------------------------------------
 1      74      Te 1/0/49:1     0      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      76      Te 1/0/49:2     1      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      80      Te 1/0/49:3     3      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
 1      78      Te 1/0/49:4     2      Te 48/0/49      XX:XX:XX:XX:XX:XX:XX:XX
```

Related Commands

fabric trunk enable, show fabric isl, show fabric islports

show fcoe fabric-map

Displays the FCoE fabric-map configuration globally in a fabric, or on a single RBridge.

Syntax

show fcoe fabric-map [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To display the fabric-map configuration on all RBridges in the fabric:

```
switch# show fcoe fabric-map

================================================================================
Fabric-Map         VLAN    VFID    Pri  FCMAP      FKA     Timeout
================================================================================
default            1002[D] 128[D]  3[D] 0xefc00[D] 8000[D] Enabled[D]
```

To display the fabric-map configuration for a single RBridge:

```
switch# show fcoe fabric-map rbridge-id 19
================================================================================
Fabric-Map            VLAN     VFID     Pri   FCMAP       FKA      Timeout
================================================================================
default               1002[D]  128[D]   3[D]  0xefc00[D]  8000[D]  Enabled[D]
```

Related Commands

fcoe-enodes, show fcoe fcoe-enodes

show fcoe fcoe-enodes

Displays the FCoE enodes information for all or one RBridge IDs in the cluster.

Syntax

show fcoe fcoe-enodes [**rbridge-id** *number*]

Parameters

rbrige-id *number*

Defines which Rbridge ID information to display.

Modes

Privileged EXEC mode

Examples

The **show fcoe fcoe-enodes** command displays the following information:

```
switch# show fcoe fcoe-enodes

=======================================================
  Rbridge-id                Fcoe-enodes
=======================================================
  1                         64[D]
  2                         70
  20                        100
  26                        250
  37                        1000
  100                       0
  Total number of fcoe-enodes in the cluster = 1484
```

The **show fcoe fcoe-enodes rbridge-id** command displays the following information:

```
switch# show fcoe fcoe-enodes rbridhe-id  20

=======================================================
  Rbridge-id                Fcoe-enodes
=======================================================
  20                        100
  Total number of fcoe-enodes in the cluster = 100.
```

History

Release version	Command history
Network OS v5.0.0	This command was introduced.

Related Commands

show fcoe fabric-map, fcoe-enodes

show fcoe interface

Displays a synopsis of the FCoE interfaces.

Syntax

show fcoe interface [**brief** | **ethernet** [**rbridge-id** *rbridge-id*]]

Parameters

brief

Displays a brief synopsis of the configuration status.

ethernet

Displays the FCoE Ethernet Interface information.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show fcoe interface brief

================================================================================
FCOE IF             Mode            Status       Binding        Num
               Config Current  Config     Proto               VN Ports
================================================================================
1/12/1         VF     VF       Up         Down   Te 12/0/1      0
1/12/2         VF     VF       Up         Down   Te 12/0/2      0
1/12/3         VF     VF       Up         Down   Te 12/0/3      0
1/12/4         VF     VF       Up         Down   Te 12/0/4      0
1/12/5         VF     VF       Up         Down   Te 12/0/5      0
1/12/6         VF     VF       Up         Down   Te 12/0/6      0
1/12/7         VF     VF       Up         Down   Te 12/0/7      0
1/12/8         VF     VF       Up         Down   Te 12/0/8      0
1/12/9         VF     VF       Up         Down   Te 12/0/9      0
1/12/10        VF     VF       Up         Down   Te 12/0/10     0
1/12/11        VF     VF       Up         Down   Te 12/0/11     0
1/12/12        VF     VF       Up         Down   Te 12/0/12     0
1/12/13        VF     VF       Up         Down   Te 12/0/13     0
1/12/14        VF     VF       Up         Down   Te 12/0/14     0
1/12/15        VF     VF       Up         Down   Te 12/0/15     0
```

show fcoe login

Displays FCoE login information.

Syntax

show fcoe login { **interface** [**WORD** | **VN-Num** | **rbridge** | **port**] } { **rbridge-id** *rbridge-id* } { **vfid** *vf_id* } { **vlan** *vlan_id* }

Parameters

interface
Displays logins for an FCoE interface

WORD
Displays Word information.

VN-Num
Displays VN-Num information.

rbridge
Displays RBridge information.

port
Displays port information.

rbridge-id *rbridge-id*
Displays FCoE logins for a given RBridge ID.

vfid *vf_id*
Displays logins for an FCoE virtual fabric. Valid values range from 1 through 4096.

vlan *vlan_id*
Displays logins for an FCoE VLAN.

Modes

Privileged EXEC mode

Usage Guidelines

NOTE
The FCoE virtual fabric is not to be confused with the Virtual Fabrics feature that supports service or transport VFs.

show fcoe map

Displays all FCoE maps, or a single map.

Syntax

show fcoe map [**default** { **rbridge-id** *rbridge-id* } | **rbridge-id** *rbridge-id*]

Parameters

default
The fabric map name. The only map name available is "default".

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

The only map name allowed is "default."

Examples

```
switch# show fcoe map default

=================================================================
Name                DCB-Map         FABRIC-MAP(s)
=================================================================
default             default         default
```

show fcsp auth-secret dh-chap

Displays the switches (WWNs) for which a shared secret is configured.

Syntax

show fcsp auth-secret dh-chap

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Brocade VDX 6740 and Brocade VDX 2740.

Examples

```
switch# show fcsp auth-secret dh-chap
 10:00:00:05:1e:7a:c3:00
```

Related Commands

fcsp auth, fcsp auth-secret dhchap, show running-config fcsp auth

show fibrechannel login

Displays Fibre Channel logins or a specified fibrechannel interface or a specified RBridge ID..

Syntax

show fibrechannel login [*rbridge-id rbridge-id* | *interface fcoe-id*]

Parameters

rbridge-id rbridge-id
Specifies an RBridge ID.

interface fcoe-id
Specifies the FCoE interface name in VN-Num/RBridge-ID/port format of the Fibre Channbel logins to display.

Modes

Privileged EXEC mode

Examples

To view all fibrechannels:

```
sw0# show fibrechannel login
================================================================================================
Interface   Index   PID      status      protocol  speed         PortWWN
================================================================================================
Fi 17/0/3    2     110146   up(In_Sync  )  up      4G Auto     2e:83:00:05:33:26:14:26
Fi 17/0/3    2     110145   up(In_Sync  )  up      4G Auto     2d:07:00:05:33:26:14:26
Fi 17/0/3    2     110144   up(In_Sync  )  up      4G Auto     2e:fc:00:05:33:26:14:26
Fi 17/0/3    2     110143   up(In_Sync  )  up      4G Auto     20:74:00:05:33:26:14:26
Fi 17/0/3    2     110142   up(In_Sync  )  up      4G Auto     26:0a:00:05:33:26:14:26
Fi 17/0/3    2     110141   up(In_Sync  )  up      4G Auto     28:2d:00:05:33:26:14:26
Fi 17/0/3    2     110140   up(In_Sync  )  up      4G Auto     10:00:00:05:33:26:14:26
Fi 17/0/4    3     110100   up(In_Sync  )  up      4G Auto     10:00:00:05:33:26:14:27
Total number of Login(s) = 8
```

To view fibrechannel logins for an RBridge:

```
sw0# show fibrechannel login rbridge-id 17
================================================================================================
Interface   Index   PID      status      protocol  speed         PortWWN
================================================================================================
Fi 17/0/3    2     110146   up(In_Sync  )  up      4G Auto     2e:83:00:05:33:26:14:26
Fi 17/0/3    2     110145   up(In_Sync  )  up      4G Auto     2d:07:00:05:33:26:14:26
Fi 17/0/3    2     110144   up(In_Sync  )  up      4G Auto     2e:fc:00:05:33:26:14:26
Fi 17/0/3    2     110143   up(In_Sync  )  up      4G Auto     20:74:00:05:33:26:14:26
Fi 17/0/3    2     110142   up(In_Sync  )  up      4G Auto     26:0a:00:05:33:26:14:26
Fi 17/0/3    2     110141   up(In_Sync  )  up      4G Auto     28:2d:00:05:33:26:14:26
Fi 17/0/3    2     110140   up(In_Sync  )  up      4G Auto     10:00:00:05:33:26:14:26
Fi 17/0/4    3     110100   up(In_Sync  )  up      4G Auto     10:00:00:05:33:26:14:27

Total number of Login(s) = 8
```

To view fibrechannel logins on an interface:

```
sw0# show fibrechannel login interface 17/0/3
=================================================================================================
Interface   Index   PID      status      protocol  speed         PortWWN
=================================================================================================
Fi 17/0/3    2     110146   up(In_Sync  )  up      4G Auto     2e:83:00:05:33:26:14:26
Fi 17/0/3    2     110145   up(In_Sync  )  up      4G Auto     2d:07:00:05:33:26:14:26
Fi 17/0/3    2     110144   up(In_Sync  )  up      4G Auto     2e:fc:00:05:33:26:14:26
Fi 17/0/3    2     110143   up(In_Sync  )  up      4G Auto     20:74:00:05:33:26:14:26
Fi 17/0/3    2     110142   up(In_Sync  )  up      4G Auto     26:0a:00:05:33:26:14:26
Fi 17/0/3    2     110141   up(In_Sync  )  up      4G Auto     28:2d:00:05:33:26:14:26
Fi 17/0/3    2     110140   up(In_Sync  )  up      4G Auto     10:00:00:05:33:26:14:26
Total number of Login(s) = 7
```

show file

Displays the contents of a file in the local flash memory.

Syntax

show file *filename*

Parameters

filename

The name of the file to be displayed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To display the contents of the startup configuration file:

```
switch# show file startup-config-copy

diag post rbridge-id 237
no enable
!
linecard 2 LC48x10G
linecard 4 LC48x10G
class-map default
match any
!
logging rbridge-id 237
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 237
chassis-name VDX8770-4
host-name sw0
!
support rbridge-id 237
ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 172.26.3.84 public
udp-port 5000
severity-level Info
!
(Output truncated)
```

Related Commands

copy, delete, dir, rename

show fips

Displays the current FIPS configuration.

Syntax

show fips

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display whether FIPS self tests are enabled, and whether the root account is disabled.

Examples

To display the FIPS enabled status:

```
switch# show fips

FIPS Selftests: Enabled
Root account:   Disabled
```

Related Commands

fips selftests, fips zeroize, prom-access disable, unhide fips

show firmwaredownloadhistory

Displays the firmware download history for the switches.

Syntax

show firmwaredownloadhistory [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

The log records the date and time of the firmware download, the switch name, slot number, process ID and firmware version.

Use this command to display information for the local management module only.

Examples

To display the firmware download history:

```
switch# show firmwaredownloadhistory
Firmware version history
Sno  Date & Time                  Switch Name  Slot  PID    OS Version
1    Thu May  2 05:00:08 2013     sw0          0     1561   nos4.0.0
2    Wed May  1 07:44:43 2013     sw0          0     1551   nos3.0.1
```

Related Commands

show version

show firmwaredownloadstatus

Displays the firmware download activity log.

Syntax

show firmwaredownloadstatus [**brief**] [**summary**] [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

brief

Displays only the last entry of the firmware download event log.

summary

Displays a high-level summary of the firmware download status.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display an event log that records the progress and status of events that occur during a firmware download. The event log is created by the **firmware download** command and is retained until you issue another **firmware download** command. A time stamp is associated with each even.t

The **rbridge-id** parameter is supported in VCS mode only.

The output varies depending on the hardware platform.

Examples

To display the firmware download event log on a Brocade VDX 8770-4:

```
switch# show firmwaredownloadstatus

[1]: Tue Mar  6 04:05:20 2012
Slot M1: Firmware install begins.

[2]: Tue Mar  6 04:09:02 2012
Slot M1: Firmware install ends.

[3]: Tue Mar  6 04:09:02 2012
Slot M2: Firmware install begins.

[4]: Tue Mar  6 04:12:08 2012
Slot M2: Firmware install ends.

[5]: Tue Mar  6 04:12:09 2012
Slot M1: Firmware starts to swap.

[6]: Tue Mar  6 04:12:09 2012
Slot M2: Firmware starts to swap.
 (Output truncated)
```

To display a condensed version of the firmware download status:

```
switch# show firmwaredownloadstatus brief

[35]: Tue Mar  6 04:23:10 2012
Slot M1: Firmware is downloaded successfully.
```

To display a high-level summary of the firmware download status:

```
switch# show firmwaredownloadstatus summary rbridge-id 1-4
Rid 1: INSTALLING
Rid 2: INSTALLED (Ready for activation)
Rid 3: COMMITING
Rid 4: COMMITED
```

Related Commands

firmware activate, firmware commit, firmware download, firmware download logical-chassis, firmware recover, firmware restore, show version

show global-running-config

Displays the global running configuration for a node.

Syntax

show global-running-config

Modes

Privileged EXEC mode

Examples

The following example shows partial output for this command:

```
switch# show global-running-config
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
no support autoupload enable
support ffdc
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server user snmpadmin1 groupname snmpadmin
snmp-server user snmpadmin2 groupname snmpadmin
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser1
snmp-server user snmpuser2
snmp-server user snmpuser3
line vty
 exec-timeout 10
!
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-save
role name admin desc Administrator
role name user desc User
aaa authentication login local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none
service password-encryption
username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role user desc User
cee-map default
 precedence 1
 priority-group-table 1 weight 40 pfc on
 priority-group-table 15.0 pfc off
 priority-group-table 15.1 pfc off
 priority-group-table 15.2 pfc off
 priority-group-table 15.3 pfc off
 priority-group-table 15.4 pfc off
 priority-group-table 15.5 pfc off
 priority-group-table 15.6 pfc off
 priority-group-table 15.7 pfc off
 priority-group-table 2 weight 60 pfc off
 priority-table 2 2 2 1 2 2 2 15.0
 remap fabric-priority priority 0
 remap lossless-priority priority 0
!
fcoe
 fabric-map default
  vlan 1002
  priority 3
  virtual-fabric 128
  fcmap 0E:FC:00
  max-enodes 64
  advertisement interval 8000
  keep-alive timeout
 !
 map default
  fabric-map default
  cee-map default
 !
```

```
!
interface Vlan 1
 shutdown
!
interface Vlan 123
 shutdown
protocol lldp
 advertise dcbx-fcoe-app-tlv
 advertise dcbx-fcoe-logical-link-tlv
 advertise dcbx-tlv
 system-description Brocade-VDX-VCS 300
!
vlan dot1q tag native
port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
!
class-map cee
class-map default
```

Related Commands

show rbridge-running config, show rbridge-local-running-config

show ha

Displays the High Availability (HA) status of the management modules.

NOTE
HA is not supported in this release. All failover is disruptive. The HA commands are provided for consistency and future expansion.

Syntax

show ha [**all-partitions**] [**rbridge-id** { *rbridge-id* } **all** }]

Parameters

all-partitions
Displays the HA status for all partitions.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

If a failover becomes necessary while the management modules are not in sync, the standby management module reboots, and the failover is disruptive.

Command Output

The **show ha** command displays the following information:

Output field	Description
Local MM state	warm or cold, recovering or recovered
Remote MM state	warm or cold, recovering or recovered, or not available
High Availability	enabled or disabled
Heartbeat	up or down
Health of standby management module	The health of the standby CP is defined as follows: • Healthy—The standby management module is running and the background health diagnostic has not detected any errors. • Failed—The standby is running, but the background health diagnostic has discovered a problem with the blade. Check the logs to determine the appropriate action.

Output field	Description
	• Unknown—The standby management module's health state is unknown because of one of the following reasons: the standby CP does not exist, Heartbeat is down, or the Health Monitor has detected a configuration file error.
HA synchronization status	The High Availability synchronization status is defined as follows: • HA State synchronizedThe system is fully synchronized. If a failover becomes necessary, it is non-disruptive. • HA State not in sync—The system is unable to synchronize the two management modules. This may be caused by one or more of the following conditions: – A failover is in process but not completed. – The standby management module is faulty. – A system error occurred.

Examples

To display HA status:

```
switch# show ha

Local (M2): Active, Cold Recovered
Remote (M1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

To display HA status for all partitions:

```
switch# show ha all-partitions
Local (M2): Active, Cold Recovered
Remote (M1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
L2/0: Active, Cold Recovered, Dual Partitions, Redundant, State in sync
   1: Standby, Dual Partitions, Redundant, State in sync
```

Related Commands

ha disable, ha enable, ha failover

show hardware connector-group

Displays all of the connector groups and the corresponding flexports in the groups.

Syntax

show hardware connector-group

Modes

Privileged EXEC mode

Examples

The **show hardware connector-group** command displays the following information:

```
switch# show hardware connector-group
Connector-group    Flexports
1/0/1                      1-8
1/0/3                      17-24
1/0/5                      33-40
1/0/6                      41-48
```

History

Release version	Command history
5.0.0	This command was introduced.

show hardware-profile

Displays the route table and TCAM profiles in the running configuration, as well as the current active profile information and subtype details for each profile type and RBridge ID.

Syntax

show hardware-profile { **current** [**rbridge-id** [*rbridge-id* | **all**] | **route-table** { **default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd** } | **tcam** { **default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd** }}

Parameters

current

Displays current active profile information. This option is available only in fabric cluster mode.

rbridge-id

Specifies an RBridge ID or all RBridge IDs.

rbridge-id

Range is from 1 through 239. This option is available only in logical chassis cluster mode.

all

Specifies all RBridge IDs.

route-table

Specifies hardware resources for route profiles.

default

Specifies IPv4/IPv6 resources for dual-stack operations.

ipv4-max-route

Specifies resources for the maximum number of IPv4 routes.

ipv4-max-arp

Specifies resources for the maximum number of IPv4 ARP entries.

ipv4-min-v6

Specifies resources for IPv4 routes in dual-stack configurations.

ipv6-max-route

Specifies resources for the maximum number of IPv6 routes.

ipv6-max-nd

Specifies resources for the maximum number of IPv6 Neighbor Discovery entries.

tcam

Specifies hardware resources for TCAM profiles.

default

Specifies resources with basic support for all applications.

l2-ipv4-acl

Specifies resources for Layer 2 and IPv4 ACLs.

ipv4-v6-pbr
Specifies resources for IPv4 and IPv6 ACLs and policy-based routing tables.

ipv4-v6-qos
Specifies resources for IPv4 and IPv6 ACLs and QoS.

ipv4-v6-mcast
Specifies resources for multicast.

l2-acl-qos
Specifies resources for Layer 2 ACLs and QoS.

Modes

Privileged EXEC mode

Usage Guidelines

currentrbridge-id

Examples

The following example shows the use of the **show hardware-profile** command in fabric cluster mode, with the **current** keyword to show the results of a default profile on a Brocade VDX 6740.

```
switch# show hardware-profile current

rbridge-id: 1       switch type: BR-VDX6740

current route-table profile:                    DEFAULT
_____________________________________________
                              IPV4 Max Routes                        4096
                              Max Next-hops                             1024
                              IPV6 Max Routes                        1024
                              IPV4 Max Neighbor cache (ARPs)     16384
                              IPV6 Max Neighbor cache (ND)       4096
        IPV4 Max Multicast Routes          1024
        IPV6 Max Multicast Routes          100
        IGMP Snooping Entries                   1024
        MLD Snooping Entries                    1024
              PIM IPV4 Register Encap Entries   1024
              PIM IPV4 Register Decap Entries   1024
              PIM IPV6 Register Encap Entries   1024
              PIM IPV6 Register Decap Entries   1024
        FCoE Domain Routes and SAN routing 2048


current TCAM profile:                              DEFAULT
_____________________________________________
           LDEV_L2PSEL_SYS                         512
        LDEV_L2PSEL_FCOE                        512
        LDEV_L2PSEL_QOS                         512
        LDEV_L2PSEL_FWD                         512
           LDEV_L2PSEL_ACL                         512
        LDEV_IPV4PSEL_QOS                       512
        LDEV_IPV4PSEL_MCAST                     3072
        LDEV_IPV4PSEL_PBR                       512
        LDEV_IPV4PSEL_ACL                       512
        LDEV_L3PSEL_FCOE                        512
        LDEV_L3FWD_IPV4                         4096
        LDEV_L3FWD_FCOE                         2048
        LDEV_L3FWD_IPV6                         1024
        LDEV_L2EACL                             128
        LDEV_L2EACL_SPAN                        256
        LDEV_IPV4EACL                           512
        LDEV_FCOEEACL                           128
        LDEV_IPV4_MCUID_OVFLW                   2048
        LDEV_L2_MAC_CLASS_VID                 256
        LDEV_ING_VPN_CLASS                      4096
        LDEV_L3CTRL_CLASS                       128
        LDEV_TYPE_VLAN_CLASS                    256
```

History

Release version	Command history
Network OS v5.0.0	This command was introduced.

show history

Displays the history of commands executed on the switch.

Syntax

show history [*number*]

Parameters

number

The number of commands to display. If you omit this value, all commands are displayed.

Modes

Privileged EXEC mode

Examples

Typical command output display.

```
switch# show history
21:10:20 -- show arp vrf test
21:35:57 -- show ip
21:38:03 -- show arp vrf name
21:38:14 -- show access-
21:39:07 -- show access-list-log
21:39:18 -- show capture
21:48:53 -- show b int po
21:48:57 -- show bp
21:53:12 -- show cli
21:53:46 -- show cli
21:54:37 -- show cli
22:05:36 -- show confd-state cli listen ssh ip port
```

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for a specific interface.

Syntax

show interface [**fibrechannel** *rbridge-id/slot/port* | **management** *rbridge-id/slot/port* | **fcoe** [*vn-number/rbridge-id/front-port-number* | **rbridge-id** *rbridge-id*] | <*N*>**gigabitethernet** *rbridge-id/slot/port* | **loopback number** | **port-channel** *number* | **stats** *rbridge-id/slot/port* | **switchport** | **vlan** *vlan_id* }

Parameters

fibrechannel

See **show interface FibreChannel**.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *number*

Specifies a loopback interface.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

management

See **show interface management**.

fcoe

Specifies FCoE interfaces.

vn-number

Specifies the VN number for FCoE.

rbridge-id

Specifies an RBridge ID.

front-port-number

Specifies the front port number.

rbridge-id*rbridge-id*

Specifies an RBridge ID.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies to display the port-channel number. Valid values range from 1 through 63.

stats

See **show interface stats**.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

switchport

Specifies to display information for Layer 2 interfaces.

vlan *vlan_id*

Specifies a VLAN interface.

Modes

Privileged EXEC mode

Usage Guidelines

If **show interface loopback** is executed in logical chassis cluster mode, loopback interfaces are not shown.

Examples

To display detailed information for the 10-gigabit Ethernet interface 1/0/1:

```
switch# show interface tengigabitethernet 1/0/1

Ten Gigabit Ethernet 1/0/1 is admin down, line protocol is down (admin down)
Hardware is Ethernet, address is 0005.1e76.1aa5
Current address is 0005.1e76.1aa5
Pluggable media present, Media type is sfp
Wavelength is 850 nm
Interface index (ifindex) is 67174401
MTU 2500 bytes
LineSpeed: 10000 Mbit, Duplex: Full
Flowcontrol rx: on, tx: on
Last clearing of show interface counters: 00:02:18
Queueing strategy: fifo
Receive Statistics:
0 packets, 0 bytes
Unicasts: 0, Multicasts: 0, Broadcasts: 0
64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
Over 1518-byte pkts(Jumbo): 0
Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
Errors: 0, Discards: 0
Transmit Statistics:
0 packets, 0 bytes
Unicasts: 0, Multicasts: 0, Broadcasts: 0
Underruns: 0
Errors: 0, Discards: 0
Rate info:
Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:02:17
```

To display detailed information for a 1-gigabit Ethernet interface:

```
switch# show interface gigabitethernet 1/0/2

Gigabit Ethernet 1/0/2 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.1e76.1aa5
Current address is 0005.3313.ac7f
Fixed copper RJ-45 media present
Interface index (ifindex) is 4697661440
MTU 2500 bytes
LineSpeed: 1000 Mbit, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 1d12h37m
Queueing strategy: fifo
Receive Statistics:
0 packets, 0 bytes
Unicasts: 0, Multicasts: 0, Broadcasts: 0
64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
Over 1518-byte pkts(Jumbo): 0
Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
Errors: 0, Discards: 0
Transmit Statistics:
4425 packets, 513300 bytes
Unicasts: 4425, Multicasts: 0, Broadcasts: 0
Underruns: 0
Errors: 0, Discards: 0
Rate info:
Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 15:14:13
```

To display Layer 2 information for all interfaces:

```
switch# show interface switchport

Interface name          : Ten Gigabit Ethernet 1/0/8
Switchport mode         : access
Ingress filter          : enable
Acceptable frame types  : all
Default Vlan            : 1
Active Vlans            : 1
Inactive Vlans          : -
Interface name          : Ten Gigabit Ethernet 1/0/19
Switchport mode         : hybrid
Ingress filter          : enable
Acceptable frame types  : all
Default Vlan            : 1
Active Vlans            : 1
Inactive Vlans          : 100
Interface name          : Ten Gigabit Ethernet 1/0/20
Switchport mode         : trunk
Ingress filter          : enable
Acceptable frame types  : vlan-tagged only
Default Vlan            : 0
Active Vlans            : 1
Inactive Vlans          : -
```

Related Commands

show interface FibreChannel, show interface management, show ip interface

show interface description

Displays the interface description.

Syntax

show interface description [**rbridge-id** *rbridge-id* | *range* | **all**]

Parameters

rbridge-id *rbridge-id*

The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.

range

A range of *rbridge-id* values. The range string can be discontiguous, such as "1-3,5".

all

Selects all of the members of the logical chassis cluster.

Modes

Privileged EXEC mode

Examples

Typical command output:

```
switch# show interface description
--------------------------------------------------------------------------------
Port             Type   Speed   Description
--------------------------------------------------------------------------------
Te 1/0/1         eth    10G     appcl12-c9c06-a05-swid1105-m1-sw
Te 1/0/2         eth    10G     --
Te 1/0/3         eth    10G     --
--------------------------------------------------------------------------------
Interface                Description
--------------------------------------------------------------------------------
Po 11                    TO:appcl12-c9c06-a06-swid1106-sw-slot104
Po 12                    TO:appcl12-c9c06-a06-swid1106-sw-slot105
```

show interface FibreChannel

Displays the up or down status of the port and of the Fibre Channel protocol, whether pluggable media are present, and additional configuration information.

Syntax

show interface FibreChannel *rbridge-id/slot/port* [**detail**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

detail
Displays detailed error and statistics counters.

Modes

Privileged EXEC mode

Usage Guidelines

This command applies only to Brocade VDX 6730 switches.

Command Output

General **show interface FibreChannel** command configuration information:

Output field	Description
LineSpeed	Actual Operating speed of the port.
PortSpeed	Fixed speed of the port.
portDisableReason	The reason the port is disabled.

Following the general information, the command displays three columns of counters. The first column shows interrupt statistics:

Output field	Description
Interrupts	Total number of interrupts.
Unknown	Interrupts that are not counted elsewhere.
Lli	Low-level interface (physical state, primitive sequences).
Proc_rqrd	Frames delivered for embedded N_Port processing.

Output field	Description
Timed_out	Frames that have timed out.
Rx_flushed	Frames requiring translation.
Tx_unavail	Frames returned from an unavailable transmitter.
Free_buffer	Free buffer available interrupts.
Overrun	Buffer overrun interrupts.
2_parity_err	Secondary transmission parity errors.
Suspended	Transmission suspended interrupts.
Parity_err	Central memory parity errors.

The second column displays link error status block counters:

Output field	Description
Link_failure	Link failures
Loss_of_sync	Synchronization losses
Loss_of_sig	Signal losses
Protocol_err	Protocol errors
Invalid_word	Invalid words
Invalid_crc	Cyclic redundancy errors
Delim_err	Delimiter errors
Address_err	Addressing errors
Lr_in	Line resets in
Li_out	Line resets out
Ols_in	Offline primitive sequences in
Ols_out	Offline primitive sequences out

The third column shows the number of transmitted frames rejected and busied:

Output field	Description
Frjt	Transmitted frames rejected.
Fbsy	Transmitted frames busied.

After this, some transmission rate Information is displayed:

Output field	Description
Bandwidth	Bandwidth of the port.
Tx performance	Bytes per second transmitted.
Rx performance	Bytes per second received.

When used with the **detail** parameter, this command also reports the following receive statistics, transmit statistics, error statistics, and port error information.

Output field	Description
stat_wrx	4-byte words received.

Output field	Description
stat_frx	Frames received.
stat_c2_frx	Class 2 frames received.
stat_c3_frx	Class 3 frames received.
stat_lc_rx	Link control frames received.
stat_mc_rx	Multicast frames received.
stat_wtx	4-byte words transmitted.
stat_ftx	Frames transmitted.
stat_mc_tx	Multicast frames transmitted.
tim_txcrd_z	The number of times that the port was unable to transmit frames because the transmit buffer-to-buffer (BB) credit was zero. The purpose of this statistic is to detect congestion or a device affected by latency. This parameter is sampled at intervals of 2.5 microseconds, and the counter is incremented if the condition is true. Each sample represents 2.5 microseconds of time with 0 Tx BB Credit. An increment of this counter means that the frames could not be sent to the attached device for 2.5 microseconds, indicating degraded performance.
er_enc_in	Encoding errors inside frames.
er_crc	Frames with cyclic redundancy check (CRC) errors.
er_trunc	Frames shorter than the minimum frame length.
er_toolong	Frames longer than the maximum frame length.
er_bad_eof	Frames with bad end-of-frame.
er_enc_out	Encoding error outside frames.
er_bad_os	Invalid ordered sets (platform-specific and port-specific).
er_rx_c3_timeout	Receive class 3 frames received at this port and discarded at the transmission port due to timeout (platform-specific and port-specific).
er_tx_c3_timeout	Transmit class 3 frames discarded at the transmission port due to timeout (platform-specific and port-specific).
er_c3_dest_unreach	Class 3 frames discarded because the transmit port, although it is determined, cannot send the frame at the moment when the error occurs.
er_other_discard	Other discards due to route lookup failures or other reasons.
er_type1_miss	FCR frames with transmit errors.
er_type2_miss	Frames with routing errors.
er_type6_miss	FCR frames with receive errors.
er_zone_miss	Frames discarded due to hard zoning miss. Hardware zoning enforcement is not supported currently.
er_lun_zone_miss	Frames discarded due to zoning miss. LUN zoning is not supported currently.
er_crc_good_eof	CRC errors with good end-of-frame (EOF).
er_inv_arb	Invalid ARBs.
Loss_of_sync	Link synchronization errors.
Loss_of_sig	Link loss-of-signal errors.
Frjt	Transmitted frames rejected.
Fbsy	Transmitted frames busied.

Buffer information:

Output field	Description
Lx Mode	• L0—Link not in long-distance mode.

Output field	Description
	• LD—Link is from 5 km through 10 km. • LE—Distance is determined dynamically. • LS—Distance is determined statically by user.
Max/Resv	Buffers The maximum or reserved number of buffers that are allocated to the port based on the estimated distance (as defined by the desire-distance command). If the port is not configured in long distance mode, some systems might reserve buffers for the port. This field then displays the number of buffers reserved for the port.
Buffer Usage	The actual number of buffers allocated to the port. In LD mode, the number is determined by the actual distance and the user-specified desired distance (as defined by the desired-distance command).
Needed Buffers	The number of buffers needed to utilize the port at full bandwidth (depending on the port configuration). If the number of Buffer Usage is less than the number of Needed Buffers, the port is operating in the buffer limited mode.
Link Distance	For L0 (not in long distance mode), the command displays the fixed distance based on port speed, for instance: 10 km (1 Gbps), 5 km (2 Gbps), 2 km (4 Gbps), or 1 km (8 Gbps). For static long distance mode (LE), the fixed distance of 10 km displays. For LD mode, Brocade switches use a proprietary algorithm to estimate distance across an ISL. LD mode supports distances up to 500 km. Distance measurement on a link longer than 500 km might not be accurate. If the connecting port does not support LD mode, is shows "N/A".
Remaining Buffers	The remaining (unallocated and reserved) buffers in a port group.

NOTE

A hyphen in one of the Buffer information display fields indicates that no relevant information is available; there may be no connection to a port, or the port is disabled, or the port is not an E_Port.

Examples

To view Fibre Channel port statistics:

```
switch# show interface FibreChannel 66/0/1
fibrechannel 66/0/1 is up. Protocol state is up (connected)
Pluggable media present
LineSpeed Actual: 400,800_MB/s
PortSpeed: N8Gbps
portDisableReason: None
PortId: 427900
PortIfId: 4302303f
PortWwn: 20:79:00:05:33:67:26:78
Distance: normal
Last clearing of show interface counters: 00:00:00
Interrupts: 0 Link_failure: 0 Frjt: 0
Unknown: 0 Loss_of_sync: 1 Fbsy: 0
Lli: 9 Loss_of_sig: 2
Proc_rqrd: 5 Protocol_err: 0
Timed_out: 0 Invalid_word: 0
Rx_flushed: 0 Invalid_crc: 0
Tx_unavail: 0 Delim_err: 0
Free_buffer: 0 Address_err: 0
Overrun: 0 Lr_in: 1
Suspended: 0 Lr_out: 1
Parity_err: 0 Ols_in: 0
2_parity_err: 0 Ols_out: 1
Rate info:
Bandwidth: 8.00G
Tx performance: 0 B/sec
Rx performance: 0 B/sec
```

To view Fibre Channel port statistics details:

```
switch# show interface FibreChannel 66/0/1 detail
fibrechannel 66/0/1 is up. Protocol state is up (connected)
Pluggable media present
LineSpeed Actual: 400,800_MB/s
portSpeed: N8Gbps
portDisableReason: None
portId 423100
portIfId: 43020026
portWwn: 20:31:00:05:33:6f:27:57
Distance normal
Last clearing of show interface counters: 00:00:00
Rx Statistics:
stat_wrx 118 4-byte words received
stat_frx 4 Frames received
stat_c2_frx 0 Class 2 frames received
stat_c3_frx 0 Class 3 frames received
stat_lc_rx 2 Link control frames received
stat_mc_rx 0 Multicast frames received
Tx Statistics:
stat_wtx 282 4-byte words transmitted
stat_ftx 12 Frames transmitted
stat_mc_tx 0 Multicast frames transmitted
tim_txcrd_z 2881 Time TX Credit Zero (2.5Us ticks)
tim_txcrd_z_vc 0- 3: 2881 0 0 0
tim_txcrd_z_vc 4- 7: 0 0 0 0
tim_txcrd_z_vc 8-11: 0 0 0 0
tim_txcrd_z_vc 12-15: 0 0 0 0
Error Statistics
er_enc_in 0 Encoding errors inside of frames
er_crc 0 Frames with CRC errors
er_trunc 0 Frames shorter than minimum
er_toolong 0 Frames longer than maximum
er_bad_eof 0 Frames with bad end-of-frame
er_enc_out 0 Encoding error outside of frames
er_bad_os 1 Invalid ordered set
er_rx_c3_timeout 0 Class 3 receive frames discarded due to timeout
er_tx_c3_timeout 0 Class 3 transmit frames discarded due to timeout
er_c3_dest_unreach 0 Class 3 frames discarded due to destination
er_type2_miss 0 frames with FTB Type 2 miss
er_type6_miss 0 frames with FTB type 6 miss
er_zone_miss 0 frames with hard zoning miss
er_lun_zone_miss 0 frames with LUN zoning miss
er_crc_good_eof 0 Crc error with good eof
er_inv_arb 0 Invalid ARB
Port Error Info:
Loss_of_sync:1
Loss_of_sig:2
Frjt:0
Fbsy:0
Buffer Information:
Lx Max/Resv Buffer Needed Link Remaining
Mode Buffers Usage Buffers Distance Buffers
=================================================================
- 8 0 0 - 924
Rate info:
Bandwidth: 8.00G
Tx performance: 0 B/sec
Rx performance: 0 B/sec
```

Related Commands

show running-config interface FibreChannel

show interface management

Displays information related to a management interface.

Syntax

show interface management [*rbridge-id/port*] [**ip** [**address** | **gateway-address**] | **ipv6** [**ipv6-address** | **ipv6-gateways**] [**line-speed**]

Command Default

This command is executed on the local switch.

Parameters

rbridge-id/port
Specifies the management interface to be configured as the *rbridge-id* followed by a slash (/) and the port number.

port
On standalone platforms, the port number for the management port is always 0.On a modular switches with two redundant management modules, you can configure two management ports: 1 and 2.

ip
Displays the IPv4 configurations for the selected interface.

address
Displays assigned IPv4 addresses.

gateway-address
Displays assigned IPv4 gateway addresses.

ipv6
Displays the IPv6 configurations for the selected interface.

ipv6-address
Displays assigned IPv6 addresses.

ipv6-gateways
Displays assigned IPv6 gateway addresses.

line-speed
Displays Ethernet speed and other line configurations for the selected interface.

Modes

Privileged EXEC mode

Usage Guidelines

The address field indicates if DHCP is used to obtain an IP address or if a static IP address is used.

Examples

The following example displays information related to a management interface configured with an IPv4 address:

```
switch# show interface management

Management 2/0
ip address 10.20.49.112/20
ip gateway-address 10.20.48.1
ipv6 ipv6_address [  ]
ipv6 ipv6_gateways [ fe80::21b:edff:fe0b:2400 ]
LineSpeed Actual "1000 Mbit, Duplex: Full"
LineSpeed Configured "Auto, Duplex: Full"
```

The following example displays information related to a management interface configured with a static IPv6 address:

```
switch# show interface management

interface Management 1/0
ip address 10.17.19.145/20
ip gateway-address 10.17.16.1
ipv6 ipv6-address [ "static aaaa::aaaa/64 preferred" ]
ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:3c00 fe80::21b:edff:fe0b:9000 ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
```

The following example displays information related to a management interface on a Brocade VDX 8770. Interface 1/1 is configured with stateless IPv6 addresses:

```
switch# show interface management

interface Management 1/1
ip address 10.24.82.121/20
ip gateway-address 10.24.80.1
ipv6 ipv6-address [ "stateless fd00:60:69bc:64:205:33ff:fe15:f980/64 preferred" ]
ipv6 ipv6-gateways [ fe80::21b:edff:fe0f:bc00 fe80::21b:edff:fe0c:c200 ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
interface Management 1/2
ip address 10.24.82.255/20
ip gateway-address 10.24.80.1
ipv6 ipv6-address [  ]
ipv6 ipv6-gateways [  ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
```

Related Commands

interface management, show running-config interface management

show interface stats

Displays interface statistics for a variety of interfaces.

Syntax

show interface stats { **brief** [**slot** *linecard_number*] | **detail** [**interface** [<*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*] | **slot** *number*] }

Parameters

brief

Displays summary statistics.

slot *linecard_number*

Displays statistics for specified linecard.

detail

Displays detailed statistics.

interface

Displays statistics for all interfaces or specific types of interface.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel number. Valid values range from 1 through 6144.

slot *number*

Specifies a slot.

Modes

Privileged EXEC mode

Examples

To display detailed statistics on a 10-GbE interface:

```
sw0# show interface stats detail interface ten 0/24
 Interface TenGigabitEthernet 0/24 statistics (ifindex 403439639)
                                RX                                TX
            Packets             0                                 0
              Bytes             0                                 0
           Unicasts             0                                 0
         Multicasts             0                                 0
         Broadcasts             0                                 0
             Errors             0                                 0
           Discards             0                                 0
           Overruns             0       Underruns                 0
              Runts             0
            Jabbers             0
                CRC             0
       64-byte pkts             0
  Over 64-byte pkts             0
 Over 127-byte pkts             0
 Over 255-byte pkts             0
 Over 511-byte pkts             0
Over 1023-byte pkts             0
Over 1518-byte pkts             0
          Mbits/Sec      0.000000                          0.000000
         Packet/Sec             0                                 0
          Line-rate         0.00%                             0.00%
```

Related Commands

show interface, show ip interface

show interface status

Displays the interface status.

Syntax

show interface status [**rbridge-id** *rbridge-id* | *range* | **all**]

Parameters

rbridge-id *rbridge-id*

The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.

range

A range of *rbridge-id* values. The range string can be discontiguous, such as "1-3,5".

all

Selects all of the members of the logical chassis cluster.

Modes

Privileged EXEC mode

Examples

Typical command output:

```
switch# show interface status
--------------------------------------------------------------------------------
Port             Status   Vlan       Speed     Type            Description
--------------------------------------------------------------------------------
Te 1/0/1     connected    Trunk      10G       10G-SFPP-LR
Te 1/0/2     connected    1          10G       10G-SFPP-SR
Po 1         connected    Trunk      40G       --
Po 2         connected    1          20G       --
```

show interface trunk

Displays the interface trunk information.

Syntax

show interface trunk [**rbridge-id** *rbridge-id* | *range* | **all**]

Parameters

rbridge-id *rbridge-id*

The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.

range

A range of *rbridge-id* values. The range string can be discontiguous, such as "1-3,5".

all

All of the members of the logical cluster.

Modes

Privileged EXEC mode

Examples

Typical command output:

```
switch# show interface trunk
----------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------
Te 1/0/1         1-4094
Te 1/0/2         1-4094
Te 1/0/3         1-4094
Po 52            1-4094
Po 99            1-4094
Po 401          701-703,757,2200-2399
Po 403          701-703,757,2200-2399
Po 405          701-703,757,2200-2399
Po 407          701-703,757,2200-2399
```

show inventory

Displays the hardware inventory of the switch.

Syntax

show inventory [**chassis** | **fan** | **module** | **powerSupply**]

Parameters

chassis

Displays information about the chassis.

fan

Displays information about the fan.

module

Displays information about the module.

powerSupply

Displays information about the power supply.

Modes

Privileged EXEC mode

Examples

Example of typical command output

```
switch# show inventory
NAME:MM, Slot M1        DESCR:Chassis Blade module
PN:60-1002179-23        SN:BVT0417J00M
NAME:MM, Slot M2        DESCR:Chassis Blade module
PN:60-1002179-13        SN:BVT0302H00T
NAME:SFM, Slot S1       DESCR:Chassis Blade module
PN:60-1002180-12        SN:BVU0304H037
NAME:SFM, Slot S2       DESCR:Chassis Blade module
PN:60-1002180-12        SN:BVU0302H01Y
NAME:SFM, Slot S3       DESCR:Chassis Blade module
PN:60-1002560-01        SN:BVU0307H01G
NAME:LC, Slot L1        DESCR:Chassis Blade module
PN:60-1002466-17        SN:CCE0423J00P
NAME:LC, Slot L2        DESCR:Chassis Blade module
PN:60-1002466-09        SN:CCE0315H00B
NAME:LC, Slot L3        DESCR:Chassis Blade module
PN:60-1002569-01        SN:CCE0305H00G
NAME:LC, Slot L4        DESCR:Chassis Blade module
PN:60-1002181-12        SN:BVV0303H019
NAME:POWER SUPPLY 1     DESCR:Chassis PS module
PN:23-0000135-02        SN:BMM2J25G998
NAME:POWER SUPPLY 2     DESCR:Chassis PS module
PN:23-0000135-02        SN:BMM2J25G803
NAME: Chassis           DESCR:System Chassis
SID:BR-VDX8770-4        SwitchType:1000
PN:84-1001681-03        SN:BZA0305H00D
```

show ip bgp

Displays BGP information.

Syntax

show ip bgp { **summary** } [**rbridge-id** *rbridge-id*]

Parameters

summary
Displays the local autonomous system number (ASN), maximum number of routes supported, and some BGP4 statistics.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp
```

show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Syntax

show ip bgp attribute-entries [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Examples

```
switch# show ip bgp attribute-entries
```

show ip bgp dampened-paths

Displays all BGP4 dampened routes.

Syntax

show ip bgp dampened-paths [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp dampened-paths
```

show ip bgp filtered-routes

Displays BGP4 filtered routes that are received from a neighbor or peer group.

Syntax

show ip bgp filtered-routes { **detail** } [*ip-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name*] | **prefix-list** *name*] [**rbridge-id** *rbridge-id*]

Parameters

detail
Optionally displays detailed route information.

ip-addr
IPv4 address of the destination network in dotted-decimal notation.

mask
(Optional) IPv4 mask of the destination network in CIDR notation.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list
Specifies an AS-path ACL.

prefix-list
Specifies an IP prefix list.

name
Name of an AS-path ACL or prefix list.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp filtered-routes detail 10.11.12.13 prefix-list
```

show ip bgp flap-statistics

Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ip bgp flap-statistics [*ip-addr* { **/** *mask* }] [**longer-prefixes**]]] | **as-path-filter** *name*] | **neighbor** *ip-addr*] | [**regular-expression** *name*] [**rbridge-id** *rbridge-id*]

Parameters

detail
Optionally displays detailed route information.

ip-addr
IPv4 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv4 mask of a specified route in CIDR notation.

as-path-filter *name*
Specifies an AS-path filter.

longer-prefixes
Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

neighbor
Displays flap statistics only for routes learned from the specified neighbor.

ip-addr
IPv4 address of the neighbor.

regular-expression
Specifies a regular expression in the display output on which to filter.

name
Name of an AS-path filter or regular expression.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp flap-statistics neighbor 10.11.12.13
```

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors of the device.

Syntax

show ip bgp neighbors { *ip-addr* | **route-summary** | **last-packet-with-error** } [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

route-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

last-packet-with-error
Displays the last packet with an error.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP4 neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Examples

```
switch# show ip bgp neighbors route-summary
```

show ip bgp neighbors advertised-routes

Displays configuration information and statistics for BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **advertised-routes** { **detail** | *ip-addr* { **/** *mask-bits* } } [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

advertised-routes
Displays only the routes that the device has advertised to the neighbor during the current BGP4 session.

detail
Displays details of advertised routes.

mask-bits
Number of mask bits in CIDR notation.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp neighbors 10.11.12.13 advertised-routes detail
```

show ip bgp neighbors flap-statistics

Displays configuration information and flap statistics for BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **flap-statistics** [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

flap-statistics
Displays the route flap statistics for routes received from or sent to a neighbor.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp neighbors 10.11.12.13 flap-statistics
```

show ip bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **received** [**extended-community** | **prefix-filter**] [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

extended-community
Displays the results for ORFs that use the BGP Extended Community Attribute.

prefix-filter
Displays the results for ORFs that are prefix-based.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp neighbors 10.11.12.13 received extended-community
```

show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ip bgp neighbors *ip-addr* **received-routes** { **detail** } [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

detail
Displays detailed route information.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp neighbors 10.11.12.13 received-routes
```

show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** } | **detail** { **best** | **not-installed-best** | **unreachable** } [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

best
Displays routes received from the neighbor that are the best BGP4 routes to their destination.

not-installed-best
Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable
Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

detail
Displays detailed information for the specified route types.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view best-route information received in UPDATE messages:

```
switch# show ip bgp neighbors 10.11.12.13 routes best
```

show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes-summary** [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp neighbors 10.11.12.13 routes-summary
```

show ip bgp peer-group

Displays peer-group information.

Syntax

show ip bgp peer-group *peer-group-name* [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

peer-group-name
Peer-group name configured by the **neighbor** *peer-group-name* command.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP4 neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Examples

```
switch# show ip bgp peer-group mypeergroup
```

Related Commands

neighbor (BGP)

show ip bgp routes

Displays BGP4 route information that is filtered by the table entry at which the display starts.

Syntax

show ip bgp routes *num* [**rbridge-id** *rbridge-id*]

Parameters

num

Table entry at which the display starts.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show ip bgp routes 100
```

show ip bgp routes age

Displays BGP4 route information that is filtered by age, best/not best routes, or routes not installed.

Syntax

show ip bgp routes [**age** *num* | **best** | **no-best** | **cidr-only** | **not-installed-best**] [**rbridge-id** *rbridge-id*]

Parameters

age
Displays only those routes that have been received or updated more recently than the number of seconds specified by *num* .

num
Last update interval, in seconds.

best
Displays only routes received from a neighbor that the device selected as best routes.

no-best
Displays only routes received from a neighbor that the device selected as suboptimal routes.

cidr-only
Displays only routes whose network masks do not match their class network length.

not-installed-best
Displays only routes received from a neighbor that are the best BGP4 routes to their destinations, but that were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static routes).

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 best route information:

```
switch# show ip bgp routes best
```

show ip bgp routes as-path-access-list

Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL).

Syntax

show ip bgp routes [**as-path-access-list** *name*] [**rbridge-id** *rbridge-id*]

Parameters

as-path-access-list
Displays only those routes that use the AS-path ACL defined by *name* .

name
Name of AS-path ACL.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 routes filtered by AS-path ACL:

```
switch# show ip bgp routes as-path-access-list myacl
```

show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

Syntax

show ip bgp routes [**community** *num* | **internet** | **local-as** | **no-advertise** | **no-export**] [**rbridge-id** *rbridge-id*]

Parameters

community
Displays routes filtered by a variety of communities.

num
Specific community member.

internet
Displays routes for the Internet community.

local-as
Displays routes for a local sub-AS within the confederation.

no-advertise
Displays routes with this community that cannot be advertised to any other BGP4 devices at all.

no-export
Displays routes for the community of sub-ASs within a confederation.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 routes filtered by community:

```
switch# show ip bgp routes community 10
```

show ip bgp routes community-access-list

Displays BGP4 route information for an AS-path community access list.

Syntax

show ip bgp routes community-access-list *name* [**rbridge-id** *rbridge-id*]

Parameters

name
Name of the AS path community access list. Range is from 1 through 32 ASCII characters.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 route information for an AS-path community access list:

```
switch# show ip bgp routes community-access-list mycommunityacl
```

show ip bgp routes community-reg-expression

Displays BGP4 route information for an ordered community-list regular expression.

Syntax

show ip bgp routes community-reg-expression *expression* [**rbridge-id** *rbridge-id*]

Parameters

expression
An ordered community-list regular expression.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 route information for an ordered community-list regular expression:

```
switch# show ip bgp routes community-reg-expression myregexpression
```

show ip bgp routes longer-prefixes

Displays BGP4 route information that is filtered for a specific prefix and mask, as well as for prefixes with a longer mask than the one specified.

Syntax

show ip bgp routes *ip-addr/prefix* [**longer-prefixes** | *ip-addr*] [**rbridge-id** *rbridge-id*]

Parameters

ip-addr
IPv4 address in dotted-decimal notation.

prefix
Mask length in CIDR notation.

longer-prefixes
Filters on prefixes equal to or greater than that specified by the mask.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 route information filtered by longer prefixes:

```
switch# show ip bgp routes  10.11.12.12/23 longer-prefixes
```

show ip bgp routes neighbor nexthop local unreachable

Displays BGP4 route information that is filtered by neighbor, next hop, and other options.

Syntax

show ip bgp routes [**neighbor** *ip-addr* | **nexthop** *ip-addr* | **local** | **unreachable**] [**rbridge-id** *rbridge-id*]

Parameters

neighbor
Displays only those routes that are received from the specified neighbor.

nexthop
Displays only those routes that are received from the specified next hop.

ip-addr
IPv4 address of neighbor or next hop, in dotted-decimal notation.

local
Displays only those routes that use a Local AS.

unreachable
Displays only those routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 routes filtered by neighbor:

```
switch# show ip bgp routes neighbor 10.11.12.13
```

show ip bgp routes prefix-list regular-expression route-map

Displays BGP4 route information that is filtered by prefix list and other options.

Syntax

show ip bgp routes [**prefix-list** *string* | **regular-expression** *name* | **route-map** *name*] [**rbridge-id** *rbridge-id*]

Parameters

prefix-list
Displays only those routes that use the specified prefix list.

string
Identifier of IP prefix list.

regular-expression
Displays only those routes that are associated with the specified regular expression.

name
Regular expression, in quotes.

route-map
Displays only those routes that use the specified route map.

name
Name of route map.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view BGP4 routes filtered by prefix list:

```
switch# show ip bgp routes prefix-list myprefixlist
```

show ip bgp routes summary detail

Displays BGP4 summary route information.

Syntax

show ip bgp routes [**summary** | **detail**] [**rbridge-id** *rbridge-id*]

Parameters

summary
Displays summary route information.

detail
Displays detailed route information.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To view summary BGP4 route information:

```
switch# show ip bgp routes summary
```

show ip dhcp relay address interface

Displays IP DHCP Relay addresses configured on a specific interface.

Syntax

show ip dhcp relay address interface [*<N>*__gigabitethernet__ *rbridge-id/slot/port*]

show ip dhcp relay address interface ve *vlan_id* { **rbridge-id** *rbridge-id* | **all** | *range* }

Command Default

If the **rbridge-id** parameter is omitted, IP DHCP Relay addresses display for the local switch.

Parameters

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve

VE interface.

vlan_id

VLAN identification for interface.

rbridge-id *rbridge-id*

Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all

Specifies all RBridge IDs in the logical chassis cluster.

range

A range of RBridge IDs separated by a dashes or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

This command displays IP DHCP Relay addresses configured on specific physical or virtual Ethernet (VE) interfaces located on a local switch, specific switches, or all switches in a logical chassis cluster. No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5).

Examples

Display configured IP DHCP Relay addresses on a specific physical interface:

```
sw0# show ip dhcp relay address interface tengigabitethernet 1/0/24
                                Rbridge Id: 1
                                ----------------
Interface                               Relay Address                       VRF Name
-------------                 -------------                        ---------
Te 1/0/24                             10.3.4.5                            default-vrf
Te 1/0/24                                10.5.1.1                             blue
```

Display configured IP DHCP Relay addresses on VE interface for RBridge ID 1.

```
sw0# show ip dhcp relay addrerss int ve 300 rbridge-id 1
                                   Rbridge Id:    1
                                   ----------------
Interface              Relay Address            VRF Name
------------           --------------        --------
Ve 300                          10.0.1.2               default-vrf
```

Display configured IP DHCP Relay addresses on VE interface on RBridge IDs 1 and 3.

```
sw0# show ip dhcp relay address interface ve 300 rbridge-id 1,3
                                   Rbridge Id:    1
                                   ----------------
Interface                Relay Address                          VRF Name
---------                -------------                          --------
Ve 300                                10.0.1.2                             default-vrf
                                   Rbridge Id:    3
                                   ----------------
Ve 300                                10.0.0.5                             default-vrf
```

Related Commands

ip dhcp relay address, show ip dhcp relay address rbridge-id

show ip dhcp relay address rbridge-id

Displays IP DHCP Relay addresses.

Syntax

show ip dhcp relay address rbridge-id *rbridge-id* | **all** | *range*

Command Default

If the *rbridge-id* parameter is omitted, IP DHCP Relay addresses display for the local switch.

Parameters

rbridge-id

Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all

Specifies all RBridge IDs in the logical chassis cluster.

range

A range of RBridge IDs separated by a dashes or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the IP address and Virtual Routing and Forwarding (VRF) name for all interfaces with configured IP DHCP Relay addresses on a local switch, specific switches, or all switches in a VCS Fabric cluster. No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5).

Examples

To display addresses configured on a specific RBridge ID:

```
sw0# show ip dhcp relay address rbridge-id 2
                                Rbridge Id:    2
                                ----------------
Interface                                Relay Address             VRF Name
-------------     -------------            ---------
Te 2/2/1                  10.1.1.1                                      Blue
Te 2/4/2                                     20.1.1.1                                    Blue
Te 2/5/4                                     30.1.1.1                                       Default-vrf
Te 2/6/6                                     40.1.1.1                                       Green
```

To display addresses configured on all switches in a virtual fabric cluster:

```
sw0# show ip dhcp rel address rbridge-id all
                                Rbridge Id:    1
                                -------------
Interface                                Relay Address                                VRF Name
---------                                -------------                                --------
Te 1/0/24                                2.3.4.5                                      default-vrf
Ve 300                                   10.0.1.2                                     default-vrf
                                Rbridge Id:    3
                                -------------
Interface                                Relay Address                                VRF Name
---------                                -------------                                --------
Ve 300                                   10.0.0.5                                     default-vrf
```

Related Commands

ip dhcp relay address, show ip dhcp relay address interface

show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

Syntax

show ip dhcp relay statistics [**ip-address** *ip-addr*] [**rbridge-id** *rbridge-id* | **all** | *range*]

Command Default

If the **rbridge-id** parameter is omitted, IP DHCP Relay statistics display for the local switch. If the **ip-address** parameter is omitted, statistics display for all configured addresses on defined switches.

Parameters

ip-address *ip-addr*

IPv4 address of DHCP server where client requests are to be forwarded.

rbridge-id *rbridge-id*

Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all

Specifies all RBridge IDs in the logical chassis cluster.

range

A range of RBridge IDs separated by a dashes or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster. To display addresses for configured interfaces on a local switch, an RBridge ID parameter is not required.

The **show ip dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on a local switch, specific switches, or all switches in a logical chassis cluster:

- DHCP Server IP Address configured in the switch.
- Number of DHCP DISCOVERY, OFFER, REQUEST, ACK, NAK, DECLINE, and RELEASE packets received.
- Number of DHCP client packets received (on port 67) and relayed by the Relay Agent.
- Number of DHCP server packets received (on port 67) and relayed by the Relay Agent.

Examples

To display statistics for a local switch:

```
switch# show ip dhcp relay statistics
DHCP Relay Statistics - Rbridge Id: 3
---------------------------------------
Address             Disc. Offer                 Req.         Ack         Nak         Decline
Release    Inform
-------             -----     -----             ----         ---         ---         -------
-------                 -------
10.1.0.1             400         100                 2972            2968
0                     0                                 0                                                 0
20.2.0.1             400         100                 2979            2975         0
0                                  0                                                 0
30.3.0.1             400         100                 3003            2998         0
0                                  0                                                 0
40.4.0.1             400         100                 3026            3018         0
0                                  0                                                 0
Active Clients: 400
Clients to Restore: 0
Client Packets: 12780
Server Packets: 12359
Timed Out: 0
No Offers: 0
```

To display statistics for specific RBridge IDs:

```
switch# show ip dhcp relay statistics rbridge-id 1,3
DHCP Relay Statistics - Rbridge Id: 1
---------------------------------------
Address             Disc. Offer                 Req.         Ack         Nak         Decline
Release            Inform
-------             -----     -----             ----         ---         ---         -------
-------                    -------
2.3.4.5                   300         100                    1211         2968         0
0                          0                                 0
10.0.1.2                 300         100                    1207         2975         0
0                          0                                 0
Client Packets: 2701
Server Packets: 2932

DHCP Relay Statistics - Rbridge Id: 3
---------------------------------------
Address             Disc. Offer                 Req.         Ack         Nak         Decline
Release    Inform
-------             -----     -----             ----         ---         ---         -------
-------                 -------
10.0.0.5                  0                 0                                 0
0              0                      0
0                                    0
10.0.1.2                  0                 0                                 0
0              0                      0
0                                    0
Client Packets: 0
Server Packets: 0
```

Related Commands

show ip dhcp relay address interface, show ip dhcp relay address rbridge-id

show ip igmp groups

Displays information related to learned groups in the IGMP protocol module.

Syntax

show ip igmp groups [[[**A.B.C.D** [**detail**]] | **rbridge-id** { *rbridge-id* | **all** } | [*interface* [<*N*>**gigabitethernet** *rbridge-id/slot/port* | **ve** [*vlan_id* | **rbridge-id** *rbridge-id*] [**detail** | *A.B.C.D*]] | [**interface vlan** *vlan_id* | **detail**] | [**interface port-channel** *number* | **detail**]]]

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

detail

Displays the IGMPv3 source information.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

all

Specifies all RBridges.

interface

Use this parameter to specify the interface.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies the virtual Ethernet (VE) interface.

detail

Displays the IGMPv3 source information.

interface

Use this parameter to specify the interface.

vlan *vlan_id*

Specifies which VLAN interface to display the snooping configuration related information.

detail

Displays the IGMPv3 source information.

interface

Use this parameter to specify the interface.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

detail

Displays the IGMPv3 source information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the IGMP database, including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

The remote RBridge information is not displayed when the detail and interface operands are used.

In logical chassis mode, when **rbridge-id** is specified, groups learned on Layer 3 interfaces for that particular RBridge ID are displayed. However, groups learned on Layer 2 interfaces from all the nodes in an entire cluster are displayed.

In logical chassis mode, if **rbridge-id** is not specified, IGMP groups on Layer 3 interfaces of the node on which the command is executed are displayed. Groups learned on Layer 2 interfaces from all the nodes in the cluster are displayed.

In logical chassis mode, when **rbridge-id all** is specified, all groups from all the nodes in the cluster are displayed.

Examples

This is an example of a detailed output.

```
switch# show ip igmp groups interface tengigabitethernet 125/1/32 detail

Interface:  Te 125/1/32
Group:  225.225.1.1
Uptime:  00:02:45
Expires:  00:03:56
Last reporter:  125.32.1.3
Last reporter mode:  IGMP V2
```

This is an example of a virtual interface output.

```
switch# show ip igmp groups interface ve 2006

Total Number of Groups: 1
IGMP Connected Group Membership
Group Address   Interface   Uptime     Expires    Last Reporter
226.226.1.1     Vlan 2006   00:00:09   00:04:03   112.26.1.25
Member Ports: Te 125/2/12
```

show ip igmp interface

Displays information related to VLANs in the IGMP protocol module.

Syntax

show ip igmp interface [**vlan** *vlan_id* [[*A.B.C.D* [**detail**]] | **rbridge-id** { *rbridge-id* | **all** } | [**interface** [*<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** [*vlan_id* | **rbridge-id** *rbridge-id*] [**detail** | *A.B.C.D*]] | [**interface vlan** *vlan_id* | **detail**] | [**interface port-channel** *number* | **detail**]]]

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

detail

Displays the IGMPv3 source information.

rbridge-id *rbridge-id*

Specifies an RBridge.

all

Specifies all RBridges.

interface

Use this parameter to specify the interface.

vlan *vlan_id*

Specifies a VLAN interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies a Virtual Ethernet (VE) interface.

detail

Displays the IGMPv3 source information.

interface

Use this parameter to specify the interface.

detail

Displays the IGMPv3 source information.

interface

Use this parameter to specify the interface.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

detail

Displays the IGMPv3 source information.

Modes

Privileged EXEC mode

Usage Guidelines

In logical chassis mode:

- When the **rbridge-id** option is specified, details for the VE interface on that particular rbridge are displayed.
- If **rbridge-id** is not specified, details for the VE interface on the node on which the command is executed is displayed.
- When **rbridge-id all** is specified, all VE interfaces with that **rbridge-id** from all the nodes in the cluster are displayed.

Examples

```
switch# show ip igmp interface vlan 1

Interface Vlan 1
 IGMP Snooping disabled
 IGMP Snooping fast-leave disabled
 IGMP Snooping querier disabled
 Number of router-ports: 0
```

show ip igmp snooping

Displays IGMP snooping information.

Syntax

show ip igmp snooping [**interface vlan** *vlan_id* | **mrouter interface vlan** *vlan_id*]

Parameters

interface vlan *vlan_id*
Specifies which VLAN interface to display the snooping configuration related information.

mrouter interface vlan *vlan_id*
Specifies which VLAN interface to display the snooping configuration related information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display IGMP snooping information, display multicast router port related information for the specified VLAN, or to display snooping statistics for the specified VLAN in the IGMP protocol module.

Examples

To display IGMP snooping information for VLAN 5:

```
switch# show ip igmp snooping interface vlan 5
```

show ip igmp statistics

Displays IGMP statistics for an interface.

Syntax

show ip igmp statistics interface [**interface** *<N>***gigabitethernet** *rbridge-id/slot/port* | **vlan** *vlan_id* | **ve** *vlan_id* [**rbridge-id** *rbridge-id*]]

Parameters

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

vlan *vlan_id*
Specifies which VLAN interface to display the snooping configuration related information.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

rbridge-id *rbridge-id*
Specifies an RBridge.

Modes

Privileged EXEC mode

Usage Guidelines

In logical chassis mode:

- When the **rbridge-id** option is specified, details for the VE interface on that particular rbridge are displayed.
- If **rbridge-id** is not specified, details for the VE interface on the node on which the command is executed is displayed.
- When **rbridge-id all** is specified, all VE interfaces with that **rbridge-id** from all the nodes in the cluster are displayed.

Examples

```
switch# show ip igmp statistics interface vlan 1

IGMP packet statistics for all interfaces in Vlan 1:
IGMP Message type     Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL Received
Membership Query                  0           0                0              0
V1 Membership Report              0           0                0              0
V2 Membership Report              0           0                0              0
Group Leave                       0           0                0              0
V3 Membership Report              0           0                0              0
PIM hello                         0           0                0              0

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

show ip interface

Displays the IP interface status and configuration of all interfaces or a specified interface.

Syntax

show ip interface [**brief** [**rbridge-id** { *rbridge-id* | **all** }] | *<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id*]

Parameters

brief

Specifies to display a brief summary of IP interface status and configuration.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *number*

Specifies to display the loopback interface number. Valid values range from 1 through 255.

port-channel *number*

Specifies to display the port-channel number. Valid values range from 1 through 6144.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface (VLAN interface number).

Modes

Privileged EXEC mode

Usage Guidelines

Note the following with respect to the **show ip interface brief** command:

- The command **show ip interface brief rbridge-id** *rbridge-id* provides information about all physical, loopback, and switched virtual interfaces (SVIs) specific to the given *rbridge-id*.
- The **show ip interface brief rbridge-id all** command provides information about all physical, loopback, and SVIs for all nodes in a cluster.
- If the **rbridge-id** option is not used, information about physical, loopback, and SVIs is shown for the local node only.
- Note the following with respect to the **show ip interface loopback** command:
- The command **show ip interface loopback rbridge-id** *rbridge-id* shows the details of loopback interfaces for the given *rbridge-id*.
- The command **show ip interface loopback rbridge-id all** shows the details of loopback interfaces for all nodes in a cluster.
- If the **rbridge-id** option is not used, information about loopback interfaces is shown for the local node only.

Note the following with respect to the **show ip interface ve** command:

- The command **show ip interface ve rbridge-id** *rbridge-id* provides inform at on about SVIs specific to the given *rbridge-id*.
- The command **show ip interface ve rbridge-id all** provides inform at on about SVIs for all nodes in a cluster.

If the **rbridge-id** option is not used, information about SVIs is shown for the local node only on the Brocade VDX family of switches.

Examples

To display information about all of the interfaces in the summary format:

```
switch# show ip interface brief

Interface                   IP-Address      Status                Protocol
========                    ==========      ======                ========
Port-channel 10             unassigned      up                     down
Port-channel 11             unassigned      up                     down
Port-channel 12             unassigned      up                     down
Port-channel 13             unassigned      up                     up
Port-channel 14             unassigned      up                     down
Port-channel 15             unassigned      up                     up
Ten Gigabit Ethernet 1/0/0
 unassigned      up                    up
Ten Gigabit Ethernet 1/0/1  unassigned      up                     down
Ten Gigabit Ethernet 1/0/2  unassigned      up                     up
Ten Gigabit Ethernet 1/0/3  unassigned      up                     up
Ten Gigabit Ethernet 1/0/4  unassigned      up                     down
Ten Gigabit Ethernet 1/0/5  unassigned      up                     down
Ten Gigabit Ethernet 1/0/6  unassigned      up                     down
Ten Gigabit Ethernet 1/0/7  unassigned      up                     up
Ten Gigabit Ethernet 1/0/8  unassigned      up                     up
Ten Gigabit Ethernet 1/0/9  unassigned      up                     up
Ten Gigabit Ethernet 1/0/10 unassigned      up                     down
Ten Gigabit Ethernet 1/0/11 unassigned      up                     down
Ten Gigabit Ethernet 1/0/12 unassigned      up                     up
Ten Gigabit Ethernet 1/0/13 unassigned      up                     up
Ten Gigabit Ethernet 1/0/14 unassigned      up                     down
Ten Gigabit Ethernet 1/0/15 unassigned      up                     up
Ten Gigabit Ethernet 1/0/16 unassigned      up                     down
Ten Gigabit Ethernet 1/0/17 unassigned      up                     up
Ten Gigabit Ethernet 1/0/18 unassigned      up                     down
Ten Gigabit Ethernet 1/0/19 unassigned      up                     up
Ten Gigabit Ethernet 1/0/20 unassigned      up                     up
Ten Gigabit Ethernet 1/0/21 unassigned      up                     up
Ten Gigabit Ethernet 1/0/22 unassigned      up                     up
Ten Gigabit Ethernet 1/0/23 unassigned      up                     up
Vlan 1                      unassigned      administratively down  down
Vlan 100                    unassigned      administratively down  down
Vlan 200                    unassigned      administratively down  down
```

To display port-security status when the port-security feature is applied:

```
sw0# show ip interface brief

Interface                 IP-Address     Status Protocol
=====================================================================
Port-channel 1           unassigned        up   up
TenGigabitEthernet 0/1   unassigned        up   up
TenGigabitEthernet 0/2   unassigned  admin-down down "Port security violation"
TenGigabitEthernet 0/3   unassigned  admin-down down
TenGigabitEthernet 0/4   unassigned  admin-down down "Port security violation"
```

To display the IP interface status of a 1-gigabit Ethernet port:

```
switch# show ip interface gigabitethernet 1/0/1

Gigabit Ethernet 1/0/1 is up protocol is up
IP unassigned
Proxy Arp is not Enabled
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
```

Related Commands

show interface

show ip interface loopback

Displays loopback information for a Management Cluster.

Syntax

show ip interface loopback *id* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

id

Displays the information for the designated loopback.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Related Commands

show ip interface, show ip interface ve

show ip interface ve

Displays virtual Ethernet (VE) port information for a Management Cluster.

Syntax

show ip interface ve *id* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

id

Displays the information for the designated loopback.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Related Commands

show ip interface, show ip interface loopback

show ip ospf

Displays the OSPF state.

Syntax

show ip ospf [**vrf** *name* [**rbridge-id** { *rbridge-id* | **all** }]]

Parameters

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

When the RBridge ID is not specified, the output from the local node is displayed.

When the RBridge ID is specified, data from the corresponding specified RBridge is displayed.

When **all** is specified, data from all nodes in the cluster is displayed.

Examples

```
Switch# show ip ospf
 vrf testname
OSPF Version                    Version 2
Router Id                       0.0.0.0
ASBR Status                     No
ABR Status                      No          (0)
Redistribute Ext Routes from
Initial SPF schedule delay      0           (msecs)
Minimum hold time for SPFs      5000        (msecs)
Maximum hold time for SPFs      10000       (msecs)
External LSA Counter            0
External LSA Checksum Sum       0
Originate New LSA Counter       0
Rx New LSA Counter              0
External LSA Limit              14913080
Database Overflow Interval      0
Database Overflow State :       NOT OVERFLOWED
RFC 1583 Compatibility :        Enabled
NSSA Translator:                Enabled
Nonstop Routing:                Disabled
Originating router-LSAs with maximum metric
Condition: Always Current State: Active
Link Type: TRANSIT
Additional LSAs originated with maximum metric:
LSA Type            Metric Value
AS-External         16711680
Type 3 Summary      16711680
Type 4 Summary      16711680
```

show ip ospf area

Displays the OSPF area table in a specified format.

Syntax

show ip ospf area { *A.B.C.D* | *decimal* } **database link-state** [**advertise** *index* | **asbr** { *asbrid* | **adv-router** *rid* } | **extensive** | **link-state-id** *lid* | **network** { *netid* | **adv-router** *rid* } | **nssa** { *nsaaid* | **adv-router** *rid* } | **router** { *routerid* | **adv-router** *rid* } | **router-id** *rid* | **self-originate** | **sequence-number** *num* | **summary** { *lid* | **adv-router** *rid* }] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format. Valid values range from 0 to 2147483647.

database link-state
Displays database link-state information.

advertise *index*
Displays the link state by Link State Advertisement (LSA) index.

asbr
Displays the link state for all autonomous system boundary router (ASBR) links.

asbrid
Displays the state of a single ASBR link that you specify.

adv-router *rid*
Displays the link state for the advertising router that you specify.

extensive
Displays detailed information for all entries in the OSPF database.

link-state-id *lid*
Displays the link state by link-state ID.

network
Displays the link state by network link.

netid
Displays the link state of a particular network link that you specify.

adv-router *rid*
Displays the link state by the advertising router that you specify.

nssa
Displays the link state by not-so-stubby area (NSSA).

nsaaid
Displays the link state of a particular NSAA area that you specify.

adv-router *rid*
Displays the link state for the advertising router that you specify.

router
Displays the link state by router link.

routerid
Displays the link state of a particular router link that you specify.

adv-router *rid*
Displays the link state by the advertising router that you specify.

router-id *rid*
Displays the link state by advertising router that you specify.

self-originate
Displays self-originated link states.

sequence-number *num*
Displays the link-state by sequence number that you specify.

summary
Displays the link state summary. Can specify link-state ID or advertising router ID.

adv-router *rid*
Displays the link state for the advertising router that you specify.

vrf vrf *name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

```
switch# show ip ospf area

Number of Areas is 4
Indx Area            Type   Cost       SPFR       ABR   ASBR  LSA   Chksum(Hex)
1    10.0.0.0        normal 0          4          0     0     0     00000000
2    11.0.0.0        normal 0          3          0     0     0     00000000
3    4               nssa   120        0          0     0     0     00000000
4    6               stub   110        0          0     0     0     00000000
```

show ip ospf border-routers

Displays information about border routers and boundary routers.

Syntax

show ip ospf border-routers [*A.B.C.D*] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

A.B.C.D

Specifies the router ID in dotted decimal format.

vrf *vrf name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router.

Examples

To display information for all ABRs and ASBRs:

```
switch# show ip ospf border-routers

Index Router-ID       Router-type Next-hop-router Outgoing-interface Area
1     1.0.0.1         ABR         22.22.22.2      2/2                7
1     1.0.0.2         ABR         22.22.22.2      2/2                7
1     1.0.0.1         ASBR        22.22.22.2      2/2                7
1     1.0.0.2         ASBR        22.22.22.2      2/2                7
```

show ip ospf config

Displays OSPF configuration.

Syntax

show ip ospf config [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

vrf *vrf name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

```
switch# show ip ospf config

Router OSPF: Enabled
Redistribution: Disabled
Default OSPF Metric: 10
OSPF Auto-cost Reference Bandwidth: Disabled
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 14913080
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Enabled
Router id: 0.0.0.0
OSPF Area currently defined:
Area-ID          Area-Type Cost
0                normal    0
1                normal    0
OSPF Area Range currently defined:
Area-ID   Range-Address    Subnetmask       Status               Config-Cost
1            20.0.0.0       255.0.0.0      advertise             100
1            30.0.0.0       255.0.0.0      not-advertise          -
```

show ip ospf database

Shows database information.

Syntax

show ip ospf database [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

show ip ospf database database-summary [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

show ip ospf database external-link-state [**advertise** *index* | **extensive** | **link-state-id** *lid* | **router-id** *routerid* | **sequence-number** *num*] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

show ip ospf database link-state [**advertise** *index* | **asbr** { *asbrid* | **adv-router** *rid* } | **extensive** | **link-state-id** *lid* | **network** { *netid* | **adv-router** *rid* } | **nssa** { *nsaaid* | **adv-router** *rid* } | **router** [{ *routerid* | **adv-router** *rid* } | **router-id** *routerid* | **self-originate** | **sequence-number** *num* | **summary** { *lid* | **adv-router** *rid* }]

Parameters

database-summary

Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.

external-link-state

Displays information by external link state, based on the following parameters:

advertise *index*

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's External LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

extensive

Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *lid*

Displays external LSAs for the LSA source that you specify.

router-id *routerid*

Displays external LSAs for the advertising router that you specify.

sequence-number *num*

Displays the External LSA entries for the hexadecimal LSA sequence number that you specify.

link-state

Displays the link state, based on the following parameters:

advertise *index*

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's external-LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

asbr

Displays autonomous system boundary router (ASBR) LSAs.

extensive
Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *lid*
Displays LSAs for the LSA source that you specify.

network
Displays either all network LSAs or the LSAs for a network that you specify.

nssa
Displays either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.

router
Displays LSAs by router link.

router-id *routerid*
Displays LSAs for the advertising router that you specify.

self-originate
Displays self-originated LSAs.

sequence-number
Displays the LSA entries for the hexadecimal LSA sequence number that you specify.

summary
Displays summary information. You can specify link-state ID or advertising router ID.

adv-router *rid*
Displays the link state for the advertising router that you specify.

vrf *name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

```
switch# show ip ospf database

Link States
Index Area ID         Type LS ID           Adv Rtr         Seq(Hex) Age  Cksum
1     6               Summ 0.0.0.0         22.22.22.1      80000002 1    0xbfec
2     7               Rtr  22.22.22.1      22.22.22.1      80000002 6    0xb8cc
3     0               Summ 22.22.22.0      22.22.22.1      80000001 6    0x4294

switch# show ip ospf database

Link States
Index Area ID         Type LS ID           Adv Rtr         Seq(Hex) Age  Cksum
1     6               Summ 0.0.0.0         22.22.22.1      80000002 52   0xbfec
2     7               Rtr  22.22.22.1      22.22.22.1      80000003 7    0xda66
3     7               Rtr  1.0.0.2         1.0.0.2         80000001 1248 0xee99
4     7               Rtr  192.0.0.1       192.0.0.1       80000006 8    0x9c80
5     7               Rtr  1.0.0.1         1.0.0.1         80000001 1248 0xfe8b
6     7               Net  22.22.22.1      22.22.22.1      80000002 7    0xb419
7     7               Summ 1.0.2.0         1.0.0.1         80000001 1248 0x4314
8     7               Summ 1.0.0.0         1.0.0.1         80000001 1248 0x59ff
9     7               Summ 1.0.3.0         1.0.0.2         80000001 1248 0x3223
10    7               Summ 1.0.1.0         1.0.0.1         80000001 1248 0x4e0a
11    7               Summ 1.0.4.0         1.0.0.2         80000001 1248 0x272d
12    0               Summ 22.22.22.0      22.22.22.1      80000001 57   0x4294
13    0               ASBR 1.0.0.2         22.22.22.1      80000001 7    0x38db
14    0               ASBR 1.0.0.1         22.22.22.1      80000001 7    0x42d2
Type-5 AS External Link States
Index Age  LS ID           Router          Netmask  Metric   Flag Fwd Address
1     1248 1.0.5.0         1.0.0.1         ffffff00 00000001 0000 0.0.0.0
2     1248 1.0.8.0         1.0.0.2         ffffff00 00000001 0000 0.0.0.0
3     1248 1.0.6.0         1.0.0.1         ffffff00 00000001 0000 0.0.0.0
4     1248 1.0.7.0         1.0.0.2         ffffff00 00000001 0000 0.0.0.0
```

show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

Syntax

show ip ospf interface [{ *A.B.C.D* | *<N>***gigabitethernet** *rbridge-id/slot/port* [**brief**] | [**brief**] | **loopback** *number* | **port-channel** *number* [**brief**] | **ve** *vlan_id* [**brief**] } [**brief**]] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

A.B.C.D
Specifies interface IP address in dotted decimal format.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

brief
Displays brief summary information about the specified port.

loopback *number*
Specifies a loopback port number in the range of 1 to 255.

port-channel *number*
Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

brief
Displays brief summary information about the specified port channel.

ve *vlan_id*
Specifies the VLAN number.

brief
Displays brief summary information about the specified VLAN.

brief
Displays brief summary about all enabled interfaces.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

If the physical interface type and name are specified, the **rbridge-id** option is not available.

Examples

To display information about all enabled interfaces:

```
switch# show ip ospf interface
TenGigabitEthernet 3/0/1 admin up, oper up
IP Address 100.1.1.1, Area 0
Database Filter: Not Configured
State passive(default none), Pri 1, Cost 1, Options 2, Type broadcast Events 0
Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
DR: Router ID 0.0.0.0 Interface Address 0.0.0.0
BDR: Router ID 0.0.0.0 Interface Address 0.0.0.0
Neighbor Count = 0, Adjacent Neighbor Count= 0
Authentication-Key: None
MD5 Authentication: Key None, Key-Id None , Auth-change-wait-time 300
```

show ip ospf neighbor

Displays OSPF neighbor information.

Syntax

show ip ospf neighbor [**extensive**] { *<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **router-id** *A.B.C.D* | **ve** *vlan_id* } [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

extensive

Shows detailed information about all neighbors.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *number*

Specifies a loopback port number in the range from1 through 255.

port-channel *number*

Displays neighbor information for the specified, valid port-channel number. Valid values range from 1 through 6144.

router-id *A.B.C.D*

Displays neighbor information for the specified router ID (in dotted decimal format).

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

If the physical interface type and name are specified, the **rbridge-id** option is not available.

Examples

To show information about all OSPF neighbors:

```
switch# show ip ospf neighbor

Number of Neighbors is 2, in FULL state 1
Port  Address         Pri State      Neigh Address   Neigh ID        Ev Opt Cnt
2/2   22.22.22.1      0   FULL/OTHER 22.22.22.2      192.0.0.1       5  2   0
```

show ip ospf redistribute route

Displays routes that have been redistributed into OSPF.

Syntax

show ip ospf redistribute route [*A.B.C.D:M*] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

A.B.C.D:M
Specifies an IP address and mask for the output.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

```
switch# show ip ospf redistribute route
30.30.30.0 255.255.255.0 fwd 0.0.0.0 (0) metric 10 connected
50.1.0.0 255.255.0.0 fwd 100.1.1.100 (1) metric 10 static
```

show ip ospf routes

Displays OSPF calculated routes.

Syntax

show ip ospf routes [*A.B.C.D*] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

A.B.C.D

Specifies a destination IP address in dotted decimal format.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route.

Examples

To display all OSPF-calculated routes:

```
switch# show ip ospf routes

OSPF Regular Routes 2:
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      2.2.2.0         255.255.255.0   1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      2.2.2.1         2.2.2.1         Network   Valid      0          4000*
      Paths Out_Port        Next_Hop        Type      State
      1     eth 1/2         0.0.0.0         OSPF      00 00
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      22.22.22.0      255.255.255.0   1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      2.2.2.1         22.22.22.1      Network   Valid      0          4000*
      Paths Out_Port        Next_Hop        Type      State
      1     eth 2/2         0.0.0.0         OSPF      00 00
```

show ip ospf summary

Displays summary information for all OSPF instances.

Syntax

show ip ospf summary [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

```
switch# show ip ospf summary

Total number of OSPF instances: 1
Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
telnet@NetIron MLX-4 Router(config-ospf-router)#show ip ospf border-routers
      router ID       router type next hop router outgoing interface Area
1     1.0.0.1         ABR         22.22.22.2      2/2               7
1     1.0.0.2         ABR         22.22.22.2      2/2               7
1     1.0.0.1         ASBR        22.22.22.2      2/2               7
1     1.0.0.2         ASBR        22.22.22.2      2/2               7
```

show ip ospf traffic

Displays OSPF traffic details.

Syntax

show ip ospf traffic [{ *<N>*__gigabitethernet__ *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id* }] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *number*

Specifies a loopback port number in the range from 1 through 255.

port-channel *number*

Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

If the physical interface type and name are specified, the rbridge-id option is not available.

Examples

To show all OSPF traffic:

```
switch# show ip ospf traffic

Packets Received         Packets Sent
Hello                          10                    10
Database                       90                    89
LSA Req                        12                    11
LSA Upd                        12                    12
LSA Ack                        12                    12
No Packet Errors!
```

show ip ospf virtual

Displays information about virtual links.

Syntax

show ip ospf virtual { **link** | **neighbor** } [*index*] [[**vrf** *vrfname* [**rbridge-id** { *rbridge-id* | **all** }]] | **rbridge-id** { *rbridge-id* | **all** }]

Parameters

link *index*
Shows information about all virtual links or one virtual link that you specify.

neighbor *index*
Shows information about all virtual neighbors or one virtual neighbor that you specify.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about virtual links and virtual neighbors over virtual links. You can show information about all virtual links or virtual neighbors, or you can specify a specific virtual link or virtual neighbor.

Examples

To show information about all virtual links:

```
switch# show ip ospf virtual link
Indx         Transit Area             Router ID            Transit(sec) Retrans(sec) Hello(sec)
1                                7
192.0.0.1                        1
5                                    10
Dead(sec) events state Authentication-Key
40 0 down None
MD5 Authentication-Key: None
MD5 Authentication-Key-Id: None
MD5 Authentication-Key-Activation-Wait-Time: 300
```

To show information about all virtual neighbors:

```
switch# show ip ospf virtual neighbor
Indx         Transit Area         Router ID         Transit(sec)         Retrans(sec)     Hello(sec)
1                                 7
192.0.0.1                    1
5                                       10
Dead(sec) events state Authentication-Key
40 0 down None
MD5 Authentication-Key: None
MD5 Authentication-Key-Id: None
MD5 Authentication-Key-Activation-Wait-Time: 300
```

show ip pim bsr

Displays the Boot Strap Router (BSR) information.

Syntax

show ip pim bsr [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

The information displayed ignores whether the Protocol Independent Multicast router is the elected BSR or not.

Examples

A typical output for this command.

```
switch# show ip pim bsr

 PIMv2 Bootstrap information :
------------------------------------------------------------------
 BSR address: 10.10.10.1. Hash Mask Length 32. Priority 0.
```

Related Commands

router pim, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim group

Displays the list of multicast groups.

Syntax

show ip pim group [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a list of the multicast groups that Protocol Independent Multicast (PIM) has learned. All groups, irrespective of how PIM learned them, are displayed.

Examples

A typical output for this command.

```
switch# show ip pim group

Total number of groups: 2
1    Group 225.0.0.1
     Group member at  Te 19/2/1: Te 19/2/1
     Group member at  Ve 100: Ve 100
2    Group 225.0.0.2
     Group member at  Te 19/2/1: Te 19/2/1
     Group member at  Ve 100: Ve 100
```

Related Commands

router pim, show ip pim bsr, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim mcache

Displays the multicast cache.

Syntax

show ip pim mcache [*ip-address-1* [*ip-address-2*]] [**rbridge-id** *rbridge-id*]

Parameters

ip-address-1
Group/Source IP address

ip-address-2
Group/Source IP address

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

A typical output for this command.

```
switch# show ip pim mcache 231.0.0.10
IP Multicast Mcache TableEntry Flags : sm - Sparse Mode, ssm - Source Specific
Multicast
RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source
LRcv - Local Receiver, RegProbe - Register In Progress
RegSupp - Register Suppression Timer, Reg - Register Complete
L2Reg - L2 Registration, needRte - Route Required for Src/RPTotal entries in mcache:2001
(*, 231.0.0.10) RP 22.22.22.22 in Te 18/0/5, Uptime 00:00:56
Sparse Mode, RPT=1 SPT=0 Reg=0 L2Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1
upstream neighbor=13.13.13.1
num_oifs = 1
Ve 10, Ve 10(00:00:56/0)
Flags (0x012604a0)
sm=1 ssm=0 needRte=02   (14.14.14.100, 231.0.0.10) in Te 18/0/1, Uptime 00:00:31
Sparse Mode, RPT=0 SPT=0 Reg=0 L2Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1
upstream neighbor=48.48.48.5
  num_oifs = 1
Ve 10, Ve 10(00:00:31/0)
Flags (0x010600f5)
sm=1 ssm=0 needRte=0Number of matching entries: 2
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic

show ip pim neighbor

Displays the Protocol Independent Multicast (PIM) neighbor information.

Syntax

show ip pim neighbor [**interface** {<*N*>**gigabitethernet** | **ve** *vlan-id* } | **rbridge-id** { *rbridge-id* | **all**]

Parameters

interface

Specifies an interface.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface (VLAN interface number). Range is from 1 through 8191.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about all the neighbors that the PIM router perceives as active.

Examples

A typical output for this command:

```
switch# show ip pim neighbor

Total Number of Neighbors : 43
Port          Phy_Port    Neighbor    Holdtime   Age   UpTime        Priority
                                        sec      sec   Dd HH:MM:SS
Te 125/1/31   Te 125/1/31 125.31.1.1    105        0   00:29:30      1
Te 125/1/43   Te 125/1/43 125.49.43.2   105       20   00:29:30      1
Te 125/2/1    Te 125/2/1  125.2.1.2     105       10   00:29:40      1
Ve 2000       Ve 2000     10.1.1.5      105        0   00:27:00      1
Ve 2001       Ve 2001     21.1.1.3      105        0   00:27:00      1
Ve 2002       Ve 2002     22.1.1.131    105        0   00:27:00      1
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rpf

Displays the Reverse Path Forwarding (RPF) for a given unicast IP address.

Syntax

show ip pim rpf [*A.B.C.D* | **rbridge-id** *rbridge-id*]

Parameters

A.B.C.D
The unicast IP address.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the port that PIM regards as the best reverse path for a given unicast IP address.

The unicast IP address may be an RP address or source address.

Examples

A typical output for this command.

```
switch# show ip pim rpf 123.32.120.10

Source 123.32.120.10 directly connected on Te 1/0/21
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic

show ip pim rp-hash

Displays the Rendezvous Point (RP) information for a Protocol Independent Multicast (PIM) sparse group.

Syntax

show ip pim rp-hash [*A.B.C.D* | **rbridge-id** *rbridge-id*]

Parameters

A.B.C.D
Group address in dotted decimal format.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays all RPs for the given group. The RP address could have been learned either from the Boot Strap Router (BSR) or configured statically.

Examples

A typical output for this command.

```
switch# show ip pim rp-hash 225.125.1.1

 RP: 10.10.10.1, v2
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rp-map

Displays the Rendezvous Point (RP) to group mappings.

Syntax

show ip pim rp-map [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

A typical output for this command.

```
switch# show ip pim rp-map

Number of group-to-RP mappings: 6
Group address RP address
------------------------------
1 239.255.163.1 99.99.99.5
2 239.255.163.2 99.99.99.5
3 239.255.163.3 99.99.99.5
4 239.255.162.1 99.99.99.5
5 239.255.162.2 43.43.43.1
6 239.255.162.3 99.99.99.5
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rp-set

Displays the Rendezvous Point (RP) set list.

Syntax

show ip pim rp-set [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays information regarding all RPs that Protocol Independent Multicast (PIM) perceives. The RPs may be either statically or dynamically learned.

Examples

A typical output for this command.

```
switch# show ip pim rp-set

Static RP
---------
Static RP count: 1
   RP: 22.22.22.22
Number of group prefixes Learnt from BSR: 1
Group prefix = 231.0.0.0/4      # RPs expected: 1
      # RPs received: 1
      RP 1: 33.33.33.33    priority=0    age=10    holdtime=150
switch#
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim-sparse

Displays the internal parameters of the Protocol Independent Multicast (PIM) router or the PIM enabled interface.

Syntax

show ip pim-sparse [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* | **rbridge-id** *rbridge-id*}]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Examples

A typical output for this command.

```
switch# show ip pim-sparse
Global PIM Sparse Mode settings
 Maximum mcache: 2048 Current count: 0
 Hello interval: 30 Neighbor timeout: 105
 Join/Prune interval: 60 Inactivity interval: 180
 Hardware drop enabled: Yes Prune wait interval: 3
 Bootstrap Msg interval: 60 Candidate-RP Msg interval: 60
 Register Suppress Time: 60 Register Probe Time: 10
 Register Stop Delay: 60 Register Suppress interval: 60
 SSM Enabled: No SPT Threshold: 1
----------+-----------+-----+----+------------------+----+---------+----+------
Interface |Local      |Ver  |Mode|Designated Router |TTL |Multicast|VRF |DR
                               |Address    |      |    |Address Port      |Thr |Boundary |    |Prio
----------+-----------+-----+----+------------------+----+---------+----+------
Te 1/0/15 12.12.12.12  v2    SM   Itself             1     None      0    1
```

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim traffic

Displays the Protocol Independent Multicast (PIM) traffic statistics categorized by each PIM enabled interface.

Syntax

show ip pim traffic [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Related Commands

router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse

show ip route

Shows IP route information.

Syntax

show ip route

show ip route *A.B.C.D/M* [{ **debug** | **detail** | **longer** }]

show ip route [**all**] [**connected**] [**ospf**] [**bgp**] [**slot** *line_card_number*] [**static**] [**summary**] [**vrf** *name*] [**rbridge-id** *rbridge-id*]

show ip route nexthop [*nexthopID* [**ref-routes**]]

Parameters

A.B.C.D/M

Specifies the IPv4 address/length to show information for a specific route.

debug

Displays debug information.

detail

Displays more-specific routes with the same specified prefix.

longer

Displays routes with addresses that match the address/mask prefix.

rbridge-id

Displays routes for a selected RBridge ID.

vrf

Displays routes for a selected VRF instance.

all

Displays information for all configured ip routes.

bgp

Displays BGP route information.

connected

Displays directly connected routes, such as local Layer 3 interfaces.

nexthop

Displays information about the configured next hop.

nexthopID

Valid values range from 0 through 65535.

ref-routes

Displays all routes that point to the specified *nexthopID* .

ospf

Displays routes learned from the Open Shortest Path First (OSPF) protocol.

rbridge-id *rbridge-id*
Displays routes for a selected RBridge ID.

slot *line_card_number*
Displays information for routes with the provided line card number.

static
Displays information about the configured static routes.

summary
Displays summary information for all routes.

vrf *name*
Displays routes for a selected VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

ATTENTION
Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management. This feature is allowed only on management VRF ports.

To view the status of management routes, use the **show ip route vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually. Example output is shown below.

```
show ip route vrf mgmt-vrf

switch# show ip route vrf mgmt-vrf
Total number of IP routes: 3
Type Codes - B:BGP D:Connected O:OSPF S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port           Cost          Type Uptime
        0.0.0.0/0          10.25.224.1     mgmt 1         1/1           S    10d17h
        10.25.224.0/24     DIRECT          mgmt 1         0/0           D    10d17h
        10.25.224.18/32    DIRECT          mgmt 1         0/0           D    10d17h
```

Examples

Typical command output for basic command:

```
switch# show ip route

Total number of IP routes: 7
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    1m57s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    0m6s
3       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    1m32s
4       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    1m16s
5       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    1m13s
6       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    0m57s
7       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    0m5s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    0m5s
```

Typical command output for connected option:

```
switch# show ip route connected

Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    4m33s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    2m42s
```

Typical command output for summary option:

```
switch(config)# do show ip route summary

IP Routing Table - 7 entries:
  2 connected, 5 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS
  Number of prefixes:
  /24: 7
Nexthop Table Entry - 4 entries
```

Typical command output for static option:

```
switch(config)# do show ip route static

Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    4m27s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m11s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    4m8s
4       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    3m52s
5       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    3m0s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    3m0s
```

Typical command output for nexthop option:

```
switch# show ip route nexthop

Total number of IP nexthop entries: 4; Forwarding Use: 4
       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 277
2      0.0.0.0          Te 2/2           1/1           2147484008 191
3      0.0.0.0          Te 2/1           2/2           2147484009 302
4      1.1.1.2          Te 2/1           1/1           2147549185 190
       1.1.2.2          Te 2/2
```

Typical command output for specific ID option:

```
switch# show ip route nexthop 2147549184

       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 288
```

Typical command output for reference routes option:

```
switch# show ip route nexthop 2147549184 ref-routes

Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
       Destination        Gateway         Port        Cost          Type Uptime
1      100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m10s
2      100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m54s
3      100.1.3.0/24       1.1.1.2         Te 2/1      1
```

Typical command output for specific IP address:

```
switch# show ip route 100.1.1.1

Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
       Destination        Gateway         Port        Cost          Type Uptime
4      100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m37s
```

Typical detailed output for specific IP address:

```
switch(config)# do show ip route 100.1.1.1 detail

Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
       Destination        Gateway         Port        Cost          Type Uptime
6      100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    6m5s
       Nexthop Entry ID:2147549184, Paths: 1, Ref_Count:3/3
```

Typical command output for longer option:

```
switch# show ip route 100.0.0.0/8 longer

1      100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    14m37s
2      100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    14m21s
3      100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    14m18s
4      100.2.1.0/24       DIRECT          Te 2/1      1/1           S    14m2s
5      100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    13m10s
       100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    13m10s
```

show ip route import

Displays the IPv4 routes imported to a specified VRF

Syntax

show ip route import [**vrf** *vrf_name*] [**rbridge-id** {*rbridge-id* | **all**}]

Parameters

vrf_name

Specifies the VRF whose imported routes you want to display.

rbridge-id

Specifies a RBridge or all RBridges for the VRF whose routes you wish to display.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

To display IPv4 routes for a VRF that has been configured with the name VRF2:

```
switch# show ip route import vrf vrf2
Total number of IP routes: 106
Type Codes - B:BGP D:Connected O:OSPF S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port           Cost          Type Uptime
        12.0.0.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.1.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.2.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.3.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.4.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.5.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.6.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.7.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.8.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.9.0/24        10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.10.0/24       10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.11.0/24       10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.12.0/24       10.1.21.200     Ve 21          20/0          Be+  1m52s
        12.0.13.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.14.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.15.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.16.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.17.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.18.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.19.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
        12.0.20.0/24       10.1.22.200     Ve 22          20/0          Be+  1m52s
```

History

Release version	Command history
5.0.0	This command was introduced.

show ip route system-summary

Displays IPv4 route information with respect to route limits and next-hop limits, as well as additional information, for all VRFs and specific VRFs.

Syntax

show ip route system-summary [**rbridge-id** *rbridge-id*] [**vrf** *name*]

Parameters

rbridge-id *rbridge-id*
Displays routes for a selected RBridge ID.

vrf *name*
Displays routes for a selected VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Per-VRF data are as for the **show ip route summary vrf** command, except for all VRFs.

The **show ip route system-summary** command displays the following information:

Output field	Description
System Route Count	Displays current (all VRF aggregate) system-wide route count, the maximum value supported by the RBridge, and whether or not the system limit was exceeded in the past.
System Nexthop Count	Displays current (all VRF aggregate) system-wide next-hop count, the maximum value supported by the RBridge, and whether or not the system limit was exceeded in the past.
VRF-Name	Displays, on a per-VRF basis, the current route count on the VRF, the maximum number of routes (if configured) on the VRF, and a breakdown of routes as connected, static, per routing protocol, and so on. The display is for a named VRF, the default VRF, and the management VRF.

Examples

Typical command output:

```
switch# show ip route system-summary

System Route Count: 12192 Max routes: 20476 (Route limit not exceeded)
System Nexthop Count: 334 Max nexthops: 15360 (Nexthop limit not exceeded)

VRF-Name: 122_53
  Route count: 1033 Max routes: 2000 (Route limit not exceeded)
  18 connected, 1 static, 0 RIP, 1001 OSPF, 0 BGP, 0 ISIS

VRF-Name: abc
  Route count: 2006 Max routes: 2500 (Route limit not exceeded)
  2 connected, 0 static, 0 RIP, 2002 OSPF, 0 BGP, 0 ISIS

VRF-Name: default-vrf
  Route count: 3080 Max routes: Not Set (Route limit not exceeded)
  32 connected, 3 static, 0 RIP, 1011 OSPF, 2004 BGP, 0 ISIS

VRF-Name: mgmt-vrf
  Route count: 6 Max routes: Not Set (Route limit not exceeded)
  3 connected, 1 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS
```

History

Release version	Command history
5.0.1	This command was introduced.

show ipv6 bgp attribute-entries

Displays BGP4+ route-attribute entries that are stored in device memory.

Syntax

show ipv6 bgp attribute-entries [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4+ attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4+ route-attribute entries that are stored in device memory.

Examples

The following is sample output from the **show ipv6 bgp attribute-entries** command:

```
device# show ipv6 bgp attribute-entries

        Total number of BGP Attribute Entries: 2
1       Next Hop   : 2001::1                                MED      :1              Origin:IGP
        Originator:0.0.0.0            Cluster List:None
        Aggregator:AS Number :0            Router-ID:0.0.0.0          Atomic:None
        Local Pref:1                Communities:Internet
        AS Path    : (length 0)
        Address: 0x1205c75c  Hash:268 (0x01000000)
        Links: 0x00000000, 0x00000000
        Reference Counts: 2:0:0, Magic: 1
2       Next Hop   : ::                                     MED      :1              Origin:IGP
        Originator:0.0.0.0            Cluster List:None
        Aggregator:AS Number :0            Router-ID:0.0.0.0          Atomic:None
        Local Pref:100              Communities:Internet
        AS Path    : (length 0)
           AsPathLen: 0  AsNum: 0, SegmentNum: 0, Neighboring As: 0, Source As 0
        Address: 0x1205c7cc  Hash:365 (0x01000000)
        Links: 0x00000000, 0x00000000
        Reference Counts: 1:0:1, Magic: 2
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp dampened-paths

Displays all BGP4+ dampened routes.

Syntax

show ipv6 bgp dampened-paths [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp dampened-paths** command:

```
device# show ipv6 bgp dampened-paths

        Network               From                   Flaps     Since     Reuse     Path
*d     2001:db8:8::/45     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:1::/48     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:4::/46     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:2::/47     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:0:8000::/49     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:17::/64    2001:db8:1::1     1     0 :1 :18     0 :2 :20     100
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp filtered-routes

Displays BGP4+ filtered routes that are received from a neighbor or peer group.

Syntax

show ipv6 bgp filtered-routes { **detail** } [*ipv6-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name*] | **prefix-list** *name*] [**rbridge-id** *rbridge-id*]

Parameters

detail
Optionally displays detailed route information.

ipv6-addr
IPv6 address of the destination network in dotted-decimal notation.

mask
(Optional) IPv6 mask of the destination network in CIDR notation.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list
Specifies an AS-path ACL.

prefix-list
Specifies an IP prefix list.

name
Name of an AS-path ACL or prefix list.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp filtered-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes matching display condition	The number of routes that matched the display parameters you entered. This is the number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the left column of the display, to the left of each route. The status codes are described in the command's output. The status column displays an "IF" for each filtered route.
Prefix	The network address and prefix.
Next Hop	The next-hop router for reaching the network from the device.

Output field	Description
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for this route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The route's status, which can be one or more of the following: • A - AGGREGATE - The route is an aggregate route for multiple networks. • B - BEST - BGP4+ has determined that this is the optimal route to the destination. • b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • C - CONFED_EBGP - The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation. • D - DAMPED - This route has been dampened (by the route dampening feature), and is currently unusable. • E - EBGP - The route was learned through a in another AS. • H - HISTORY - Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. • I - IBGP - The route was learned through a in the same AS. • L - LOCAL - The route originated on this device. • M - MULTIPATH - BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. • S - SUPPRESSED - This route was suppressed during aggregation and thus is not advertised to neighbors. • F - FILTERED - This route was filtered out by BGP4+ route policies on the device, but the device saved updates containing the filtered routes.

Examples

The following is sample output from the **show ipv6 bgp filtered-routes** command:

```
device# show ipv6 bgp filtered-routes

Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix              Next Hop        MED LocPrf     Weight Status
1      2001:db8:3000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 701 80
2      2001:db8:4000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 1
3      2001:db8:5000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 701 1 189
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp flap-statistics

Displays BGP4+ route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ipv6 bgp flap-statistics [*ipv6-addr* { **/** *mask* }] [**longer-prefixes**]]] | **as-path-filter** *name*] | **neighbor** *ipv6-addr*] | [**regular-expression** *name*] [**rbridge-id** *rbridge-id*]

Parameters

detail
Optionally displays detailed route information.

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

mask
(Optional) IPv6 mask of a specified route in CIDR notation.

as-path-filter name
Specifies an AS-path filter.

longer-prefixes
Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

neighbor
Displays flap statistics only for routes learned from the specified neighbor.

ipv6-addr
IPv6 address of the neighbor.

regular-expression
Specifies a regular expression in the display output on which to filter.

name
Name of an AS-path filter or regular expression.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp flap-statistics** command displays the following information:

Output field	Description
Total number of flapping routes	The total number of routes in the device's BGP4+ route table that have changed state and thus have been marked as flapping routes.

Output field	Description
Status code	Indicates the dampening status of the route, which can be one of the following: • > - This is the best route among those in the BGP4+ route table to the route's destination. • d - This route is currently dampened, and thus unusable. • h - The route has a history of flapping and is unreachable now. • * - The route has a history of flapping but is currently usable.
Network	The destination network of the route.
From	The IPv6 address of the advertising peer.
Flaps	The number of flaps (state changes) the route has experienced.
Since	The amount of time (in hh:mm:ss) since the first flap of this route.
Reuse	The amount of time (in hh:mm:ss) after which the path is again available.
Path	The AS path of the route.

Examples

The following is sample output from the **show ipv6 bgp flap-statistics** command:

```
device# show ipv6 bgp flap-statistics

Total number of flapping routes: 14
    Status Code  >:best d:damped h:history *:valid
    Network          From           Flaps  Since    Reuse    Path
h>  2001:db8:2::/48    2001:db8:23::47  1    0 :0 :13 0 :0 :0  65001 4355 1 701
*>  2001:db8:34::/48   2001:db8:23::47  1    0 :1 :4  0 :0 :0  65001 4355 701 62
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors { *ipv6-addr* | **last-packet-with-error** | **routes-summary** } [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

last-packet-with-error
Displays the last packet with an error.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp neighbors** command when the **routes-summary** keyword is used:

```
device# show ipv6 bgp neighbors routes-summary

    Total number of BGP Neighbors: 2
1   IP Address: 2001:54:54::54
Routes Accepted/Installed:0,  Filtered/Kept:0,  Filtered:0
   Routes Selected as BEST Routes:0
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:0,  Withdraws:0 (0),  Replacements:0
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Invalid Confed aspath:0, maxas-limit aspath:0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:150,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:677,  Withdraws:512,  Replacements:15

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0

2   IP Address: 2001:55:55::55
Routes Accepted/Installed:1,  Filtered/Kept:0,  Filtered:0
   Routes Selected as BEST Routes:1
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:1,  Withdraws:0 (0),  Replacements:0
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Invalid Confed aspath:0, maxas-limit aspath:0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:150,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:677,  Withdraws:512,  Replacements:15

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors advertised-routes

Displays all the routes the BGP4+ networking device advertised to the neighbor.

Syntax

show ip bgp neighbors *ipv6-addr* **advertised-routes** { **detail** | *ipv6-addr* { **/** *mask-bits* } } [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

advertised-routes
Displays only the routes that the device has advertised to the neighbor during the current BGP4 session.

detail
Displays details of advertised routes.

mask-bits
Number of mask bits in CIDR notation.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors advertised-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes advertised to specified neighbor (appears only in display for all routes)	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The advertised route's prefix.
Next Hop	The next-hop for reaching the advertised route from the device.
MED	The value of the advertised route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference range is 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination

Output field	Description
	from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The advertised route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination. • b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • E - EBGP. The route was learned through a in another AS. • I - IBGP. The route was learned through a in the same AS. • L - LOCAL. The route originated on this device.
AS-PATH	The AS-path information for the route.

The **show ipv6 bgp neighbors advertised-routes detail** command displays the following fields that are not described in the table above:

Output field	Description
Age	The age of the advertised route, in seconds.
Learned from Peer	The IPv6 address of the neighbor from which this route is learned. "Local Router" indicates that the device itself learned the route.
MED	The value of the advertised route's MED attribute. If the route does not have a metric, this field is blank.
Origin	The source of the route information. The origin can be one of the following: • EGP - The routes with this set of attributes came to BGP4+ through EGP. • IGP - The routes with this set of attributes came to BGP4+ through IGP. • INCOMPLETE - The routes came from an origin other than one of the above. For example, they may have been redistributed from OSPFv3 or RIPng. When BGP4+ compares multiple routes to a destination to select the best route, IGP is preferred over EGP and both are preferred over INCOMPLETE.
AS-PATH	The AS-path information for the route.
Adj RIB out count	The number of routes in the device's current BGP4+ Routing Information Base (Adj-RIB-Out) for a specified neighbor.
Admin distance	The administrative distance of the route.

Examples

The following is sample output from the **show ipv6 bgp neighbors advertised-routes** command:

```
device# show ipv6 bgp neighbor 2001:54:54::54 advertised-routes

       There are 7 routes advertised to neighbor 2001:54:54::54
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      fd80:122:122:122:101:101:0:122/128  2001:122:122::122
                                           0          100        101    BL
         AS_PATH:
2      fd80:122:122:122:103:103:0:122/128  2001:122:122::122
                                           0          100        103    BL
         AS_PATH:
3      fd80:122:122:122:105:105:0:122/128  2001:122:122::122
                                           0          100        105    BL
         AS_PATH:
4      131::1/128          2001:122:122::122
                                           1          100        32768  BL
         AS_PATH:
5      2001:122:131:125:131:1::/96  2001:3002::732
                                           1          100        0      BE
         AS_PATH: 65530
6      2001:abcd:1234:1234:1:2:1:0/112  2001:3002::733
                                           1          100        0      BE
         AS_PATH: 65530
7      2001:abcd:1234:1234:1:2:2:0/112  2001:3002::733
                                           1          100        0      BE
```

The following is sample output from the **show ipv6 bgp neighbors advertised-routes** command when the **detail** keyword is used:

```
device# show ipv6 bgp neighbors 2001:54:54::54 advertised-routes detail
       There are 7 routes advertised to neighbor 2001:54:54::54
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1       Prefix: fd80:122:122:122:101:101:0:122/128,  Status: BL,  Age: 4h23m34s
         NEXT_HOP: 2001:122:122::122, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 101
         AS_PATH:
            Adj_RIB_out count: 20,  Admin distance 0
2       Prefix: fd80:122:122:122:103:103:0:122/128,  Status: BL,  Age: 4h23m32s
         NEXT_HOP: 2001:122:122::122, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 103
         AS_PATH:
            Adj_RIB_out count: 20,  Admin distance 0
3       Prefix: fd80:122:122:122:105:105:0:122/128,  Status: BL,  Age: 4h23m31s
         NEXT_HOP: 2001:122:122::122, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 105
         AS_PATH:
            Adj_RIB_out count: 20,  Admin distance 0
4       Prefix: 131::1/128,  Status: BL,  Age: 4h23m49s
         NEXT_HOP: 2001:122:122::122, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: igp,  Weight: 32768
         AS_PATH:
            Adj_RIB_out count: 20,  Admin distance 1
5       Prefix: 2001:122:131:125:131:1::/96,  Status: BE,  Age: 2h39m44s
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors flap-statistics

Displays configuration information and flap statistics for routes received from or sent to a neighbor.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **flap-statistics** [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors flap-statistics** command displays the following information:

Output field	Description
Total number of flapping routes	The total number of routes in the neighbor's BGP4+ route table that have changed state and thus have been marked as flapping routes.
Status code	Indicates the status of the route, which can be one of the following: • > - This is the best route among those in the neighbor's BGP4+ route table to the route's destination. • d - This route is currently dampened, and thus unusable. • h - The route has a history of flapping and is unreachable now. • * - The route has a history of flapping but is currently usable.
Network	The destination network of the route.
From	The IPv6 address of the advertising peer.
Flaps	The number of flaps (state changes) the route has experienced.
Since	The amount of time (in hh:mm:ss) since the first flap of this route.
Reuse	The amount of time (in hh:mm:ss) after which the path is again available.
Path	The AS path of the route.

Examples

The following is sample output from the **show ipv6 bgp neighbors flap-statistics** command:

```
device# show ipv6 bgp neighbors 2001:db8::110 flap-statistics

Total number of flapping routes: 14
    Status Code  >:best d:damped h:history *:valid
    Network            From            Flaps Since    Reuse    Path
h>  2001:db8:2::/48    10.90.213.77    1     0 :0 :13 0 :0 :0  65001 4355 1 701
*>  2001:db8:34::/48   10.90.213.77    1     0 :1 :4  0 :0 :0  65001 4355 701 62
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **last-packet-with-error** [**decode** | **rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

decode
Decodes last packet that contained an error from any of a device's neighbors.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors last-packet-with-error** command displays the following information:

Output field	Description
Total number of BGP Neighbors	The total number of configured neighbors for a device.
Last error	The error packet's contents decoded in a human-readable format or notification that no packets with an error were received.

Examples

The following is sample output from the **show ipv6 bgp neighbors last-packet-with-error** command:

```
device# show ipv6 bgp neighbor last-packet-with-error

Total number of BGP Neighbors: 67
1 IP Address: 153::2
    Last error:
    BGP4: 0 bytes hex dump of packet that contains error
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ipv6-addr* **received** [**detail** | **prefix-filter**] [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

detail
Displays detailed ORF information.

prefix-filter
Displays the results for ORFs that are prefix-based.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp neighbors received** command when the **prefix-filter** is used:

```
device# show ipv6 bgp neighbors 4001::1 received prefix-filter

ip prefix-list: 2 entries
seq 1 permit 1001::/64
seq 2 permit 4001::/64
SW0)#show ipv6 bgp neighbors 4001::1 advertised-routes
There are 2 routes advertised to neighbor 4001::1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
Prefix Next Hop MED LocPrf Weight Status
1 1001::/64 4001::2 0 100 32768 BL
AS_PATH:
2 4001::/64 4001::2 0 100 32768 BL
AS_PATH:
Taurus
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors received-routes

Lists all route information received in route updates from BGP4+ neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **received-routes** [**detail**] [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

detail
Displays detailed route information.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors received-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes received from a neighbor	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The received route's prefix.
Next Hop	The IPv6 address of the next device that is used when forwarding a packet to the received route.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The advertised route's status, which can be one or more of the following:

Output field	Description
	A - AGGREGATE. The route is an aggregate route for multiple networks. B - BEST. BGP4+ has determined that this is the optimal route to the destination. b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable. E - EBGP. The route was learned through a in another AS. H - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. I - IBGP. The route was learned through a in the same autonomous system. L - LOCAL. The route originated on this device. M - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. S - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors. F - FILTERED. This route was filtered out by BGP4+ route policies on the device, but the saved updates containing the filtered routes.

Examples

The following is sample output from the **show ipv6 bgp neighbors received-routes** command:

```
device# show ipv6 bgp neighbor 2001:db8::10 received-routes

There are 4 received routes from neighbor 2001:db8::10
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
    Prefix    Next Hop    Metric    LocPrf    Weight    Status
1     2001:db8:2002::/64    2001:db8::10     0    100    0    BE
AS_PATH: 400
2    2001:db8:2003::/64    2001:db8::10     1    100    0    BE
AS_PATH: 400
3    2001:db8:2004::/64    2001:db8::10     1    100    0    BE
AS_PATH: 400
4    2001:db8:2005::/64    2001:db8::10     1    100    0    BE
AS_PATH: 400
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors rib-out-routes

Displays information about BGP4+ outbound RIB routes.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **received-routes** [**detail**] [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

detail

Displays detailed RIB route information.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors rib-out-routes** command displays the following information:

Output field	Description
Number of RIB_out routes for a specified neighbor (appears only in display for all RIB routes)	The number of RIB routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The RIB route's prefix.
Next Hop	The next-hop router for reaching the route from the device.
MED	The value of the advertised route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The RIB route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks.

Output field	Description
	• B - BEST. BGP4+ has determined that this is the optimal route to the destination. • E - EBGP. The route was learned through a in another autonomous system. • I - IBGP. The route was learned through a in the same autonomous system. • L - LOCAL. The route originated on this device.
AS-PATH	The AS-path information for the route.

Examples

The following is sample output from the **show ipv6 bgp neighbors rib-out-routes** command:

```
device# show ipv6 bgp neighbors 2001:54:54::54 rib-out-routes

       There are 150 RIB_out routes for neighbor 2001:54:54::54
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      fd80:122:122:122:101:101:0:122/128  ::
                                           0          100        101    BL
         AS_PATH:
2      fd80:122:122:122:103:103:0:122/128  ::
                                           0          100        103    BL
         AS_PATH:
3      fd80:122:122:122:105:105:0:122/128  ::
                                           0          100        105    BL
         AS_PATH:
4      131::1/128          ::              1          100        32768  BL
         AS_PATH:
5      2001:122:131:125:131:1::/96  2001:3002::732
                                           1          100        0      BE
         AS_PATH: 65530
6      2001:abcd:1234:1234:1:2:1:0/112  2001:3002::733
                                           1          100        0      BE
         AS_PATH: 65530
7      2001:abcd:1234:1234:1:2:2:0/112  2001:3002::733
                                           1          100        0      BE
         AS_PATH: 65530
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes** { **best** | **detail** | **not-installed-best** | **unreachable** } [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

best
Displays routes received from the neighbor that are the best BGP4+ routes to their destination.

not-installed-best
Displays routes received from the neighbor that are the best BGP4+ routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable
Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

detail
Displays detailed information for the specified route types.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp neighbors routes** command when the **best** keyword is used:

```
device# show ipv6 bgp neighbor 2001:db8::106 routes best

There are 2 accepted routes from neighbor 2001:db8::106
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
Prefix Next Hop MED LocPrf Weight Status
1 2001:db8:2002::/48 2001:db8::106 1 100 0 BE
AS_PATH: 65001
2 2001:db8:2002:1234::/64 2001:db8::106 1 100 0 BE
AS_PATH: 65001
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **routes-summary** [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a specified route in dotted-decimal notation.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp neighbors routes-summary** command displays the following information:

Output field	Description
IP Address	The IPv6 address of the neighbor
Routes Received	How many routes the device has received from the neighbor during the current BGP4+ session: • Accepted or Installed - Indicates how many of the received routes the device accepted and installed in the BGP4+ route table. • Filtered or Kept - Indicates how many routes were filtered out, but were nonetheless retained in memory for use by the soft reconfiguration feature. • Filtered - Indicates how many of the received routes were filtered out.
Routes Selected as BEST Routes	The number of routes that the device selected as the best routes to their destinations.
BEST Routes not Installed in IPv6 Forwarding Table	The number of routes received from the neighbor that are the best BGP4+ routes to their destinations, but were nonetheless not installed in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes).
Unreachable Routes	The number of routes received from the neighbor that are unreachable because the device does not have a valid RIPng, OSPFv3, or static IPv6 route to the next hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.

Output field	Description
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: • Withdraws - The number of withdrawn routes the device has received. • Replacements - The number of replacement routes the device has received.
NLRIs Discarded due to	Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons: • Maximum Prefix Limit - The device's configured maximum prefix amount had been reached. • AS Loop - An AS loop occurred. An AS loop occurs when the BGP4+ AS-path attribute contains the local AS number. • Invalid Nexthop Address - The next hop value was not acceptable. • Duplicated Originator_ID - The originator ID was the same as the local router ID. • Cluster_ID - The cluster list contained the local cluster ID, or contained the local router ID (see above) if the cluster ID is not configured.
Routes Advertised	The number of routes the device has advertised to this neighbor: • To be Sent - The number of routes the device has queued to send to this neighbor. • To be Withdrawn - The number of NLRIs for withdrawing routes the device has queued up to send to this neighbor in UPDATE messages.
NLRIs Sent in Update Message	The number of NLRIs for new routes the device has sent to this neighbor in UPDATE messages: • Withdraws - The number of routes the device has sent to the neighbor to withdraw. • Replacements - The number of routes the device has sent to the neighbor to replace routes the neighbor already has.
Peer Out of Memory Count for	Statistics for the times the device has run out of BGP4+ memory for the neighbor during the current BGP4+ session: • Receiving Update Messages - The number of times UPDATE messages were discarded because there was no memory for attribute entries. • Accepting Routes(NLRI) - The number of NLRIs discarded because there was no memory for NLRI entries. This count is not included in the Receiving Update Messages count. • Attributes - The number of times there was no memory for BGP4+ attribute entries. • Outbound Routes (RIB-out) - The number of times there was no memory to place a "best" route into the neighbor's route information base (Adj-RIB-Out) for routes to be advertised. • Outbound Routes Holder - For debugging purposes only.

Examples

The following is sample output from the **show ipv6 bgp neighbors routes-summary** command:

```
device# show ipv6 bgp neighbors routes-summary

Total number of BGP Neighbors: 1
1 IP Address: 5001::1
Routes Accepted/Installed:3, Filtered/Kept:0, Filtered:0
Routes Selected as BEST Routes:3
BEST Routes not Installed in IP Forwarding Table:0
Unreachable Routes (no IGP Route for NEXTHOP):0
History Routes:0
NLRIs Received in Update Message:3, Withdraws:0 (0), Replacements:0
NLRIs Discarded due to
Maximum Prefix Limit:0, AS Loop:0
Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
Invalid Confed aspath:0, maxas-limit aspath:0
Duplicated Originator_ID:0, Cluster_ID:0
Routes Advertised:0, To be Sent:0, To be Withdrawn:0
NLRIs Sent in Update Message:0, Withdraws:0, Replacements:0
Peer Out of Memory Count for:
Receiving Update Messages:0, Accepting Routes(NLRI):0
Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp peer-group

Displays peer-group information.

Syntax

show ipv6 bgp peer-group *peer-group-name* [**rbridge-id** *rbridge-id*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

peer-group-name
Peer-group name configured by the **neighbor** *peer-group-name* command.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp peer-group** command:

```
device# # show ipv6 bgp peer-group
do show ipv6 bgp peer-group
1 BGP peer-group is P1, Remote AS: 1
Address family : IPV4 Unicast
activate
Address family : IPV4 Multicast
no activate
Address family : IPV6 Unicast
activate
Address family : IPV6 Multicast
no activate
Address family : VPNV4 Unicast
no activate
Address family : L2VPN VPLS
no activate
Members:
IP Address: 2001::1
IP Address: 2001:0:0:1::1
IP Address: 10.1.0.1
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp routes

Displays BGP4+ route information that can be filtered using various options.

Syntax

show ipv6 bgp routes [*num* | *ipv6-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community** *num* | **community-access-list** *name* | **community-reg-expression** *expression* | **detail** | **local** | **neighbor** *ipv6-addr* | **nexthop** *ipv6-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**] [**rbridge-id** *rbridge-id*]

Parameters

num
Table entry at which the display starts.

ipv6-address/prefix
Table entry at which the display starts.

age
Displays BGP4+ route information that is filtered by age.

as-path-access-list
Displays BGP4+ route information that is filtered by autonomous system (AS)-path access control list (ACL).

best
Displays BGP4+ route information that the device selected as best routes.

cidr-only
Displays BGP4+ routes whose network masks do not match their class network length.

community *num*
Displays BGP4+ route information that is filtered by community.

community-access-list *name*
Displays BGP4+ route information for an AS-path community access list.

community-reg-expression *expression*
Displays BGP4+ route information for an ordered community-list regular expression.

detail
Displays BGP4+ detailed route information.

local
Displays BGP4+ route information about selected local routes.

neighbor *ipv6-addr*
Displays BGP4+ route information about selected BGP neighbors.

nexthop *ipv6-addr*
Displays BGP4+ route information about routes that are received from the specified next hop.

no-best
Displays BGP4+ route information that the device selected as not best routes.

not-installed-best
Displays BGP4+ route information about best routes that are not installed.

prefix-list *string*
Displays BGP4+ route information that is filtered by prefix list.

regular-expression *name*
Displays BGP4+ route information about routes that are associated with the specified regular expression.

route-map *name*
Displays BGP4+ route information about routes that use the specified route map.

summary
Displays BGP4+ summary route information.

unreachable
Displays BGP4+ route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The route's prefix.
Next Hop	For normal IPv6 routes, next hop is the next hop IPv6 router to reach the destination. For the 6PE routes, next hop is the IPv4-mapped IPv6 address of the peer 6PE router.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination.

Output field	Description
	• b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • C - CONFED_EBGP. The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation. • D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable. • E - EBGP. The route was learned through a in another AS. • H - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. • I - IBGP. The route was learned through a in the same AS. • L - LOCAL. The route originated on this. • M - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. • S - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors.
AS-PATH	The AS-path information for the route.

Examples

The following is sample output from the **show ipv6 bgp routes** command:

```
device# show ipv6 bgp routes

Total number of BGP Routes: 6
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      57:7000:3:22:abc:1::/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
2      57:7000:3:22:abc:1:0:2/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
3      57:7000:3:22:abc:1:0:4/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
4      57:7000:3:22:abc:1:0:6/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
5      57:7000:3:22:abc:1:0:8/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
6      57:7000:3:22:abc:1:0:a/128  2001:700:122:57::57
                                                     100        0      BE
         AS_PATH: 7000 322
```

The following is sample output from the **show ipv6 bgp routes** command using the **summary** keyword:

```
device# show ipv6 bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 558
  Distinct BGP destination networks                : 428
  Filtered bgp routes for soft reconfig            : 0
  Routes originated by this router                 : 19
  Routes selected as BEST routes                   : 417
  BEST routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)    : 22
  IBGP routes selected as best routes              : 102
  EBGP routes selected as best routes              : 296
```

The following is sample output from the **show ipv6 bgp routes** command using the **local** keyword:

```
device# show ipv6 bgp routes local
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      131::1/128         ::              1          100        32768  BL
         AS_PATH:
2      2001:107:6133:2007:1::/112  2001:2007::201
                                          107        100        32768  BL
         AS_PATH:
3      2001:107:6133:2007:2::/112  2001:2007::202
                                          107        100        32768  BL
         AS_PATH:
4      2001:107:6133:2007:3::/112  2001:2007::203
                                          107        100        32768  BL
         AS_PATH:
5      2001:107:6133:2007:4::/112  2001:2007::204
                                          107        100        32768  BL
         AS_PATH:
6      2001:107:6133:2007:5::/112  2001:2007::205
                                          107        100        32768  BL
         AS_PATH:
7      2001:107:6133:2007:6::/112  2001:2007::206
                                          107        100        32768  BL
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 bgp summary

Displays summarized information about the status of all BGP connections.

Syntax

show ipv6 bgp summary [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 bgp summary** command displays the following information:

Output field	Description
Router ID	The device's router ID.
Local AS Number	The BGP4+ AS number in which the device resides.
Confederation Identifier	The autonomous system number of the confederation in which the device resides.
Confederation Peers	The numbers of the local autonomous systems contained in the confederation. This list matches the confederation peer list you configure on the device.
Maximum Number of Paths Supported for Load Sharing	The maximum number of route paths across which the device can balance traffic to the same destination. The feature is enabled by default but the default number of paths is 1. You can increase the number from 2 - 8 paths.
Number of Neighbors Configured	The number of BGP4+ neighbors configured on this device.
Number of Routes Installed	The number of BGP4+ routes in the device's BGP4+ route table.
Number of Routes Advertising to All Neighbors	The total of the RtSent and RtToSend columns for all neighbors.
Number of Attribute Entries Installed	The number of BGP4+ route-attribute entries in the route-attributes table.
Neighbor Address	The IPv6 addresses of this BGP4+ neighbors.
AS#	The autonomous system number.
State	The state of this neighbor session with each neighbor. The states are from this perspective of the session, not the neighbor's perspective. The state values can be one of the following for each: • IDLE - The BGP4+ process is waiting to be started. Usually, enabling BGP4+ or establishing a neighbor session starts the BGP4+ process. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes.

Output field	Description
	• ADMND - The neighbor has been administratively shut down. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • CONNECT - BGP4+ is waiting for the connection process for the TCP neighbor session to be completed. • ACTIVE - BGP4+ is waiting for a TCP connection from the neighbor. **NOTE** If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection. • OPEN SENT - BGP4+ is waiting for an Open message from the neighbor. • OPEN CONFIRM - BGP4+ has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle. • ESTABLISHED - BGP4+ is ready to exchange UPDATE packets with the neighbor. – If there is more BGP data in the TCP receiver queue, a plus sign (+) is also displayed. **NOTE** If you display information for the neighbor using the **show ipv6 bgp neighbor** command, the TCP receiver queue value will be greater than 0.
Time	The time that has passed since the state last changed.
Accepted	The number of routes received from the neighbor that this installed in the BGP4+ route table. Usually, this number is lower than the RoutesRcvd number. The difference indicates that this filtered out some of the routes received in the UPDATE messages.
Filtered	The routes or prefixes that have been filtered out. • If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP4+ route table) but retained in memory. • If soft reconfiguration is not enabled, this field shows the number of BGP4+ routes that have been filtered out.
Sent	The number of BGP4+ routes sent to the neighbor.
ToSend	The number of routes queued to send to this neighbor. • s - GR neighbor is in a stale state • r - GR neighbor is in a restarting state • < - GR neighbor is waiting for an EOR

Examples

The following is sample output from the **show ipv6 bgp summary** command:

```
device# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 122.122.122.122   Local AS Number: 122
  Confederation Identifier: not configured
  Confederation Peers:
  Cluster ID: 122
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 20, UP: 15
  Number of Routes Installed: 219, Uses 20805 bytes
  Number of Routes Advertising to All Neighbors: 2802 (440 entries), Uses 26400 bytes
  Number of Attribute Entries Installed: 31, Uses 2852 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  2001:54:54::54    122         ESTAB     0h19m58s    0        0        146      0
  2001:55:55::55    122         ESTAB     0h19m54s    1        0        146      0
  2001:122:53::53   6000        ESTAB     0h22m39s    50       0        147      0
  2001:122:534:2::534
                    534         ESTAB     0h 3m20s    10       0        137      0
  2001:125:125::125 122         CONN      0h11m33s    0        0        0       -
```

The following is sample output from the **show ipv6 bgp summary** command when a GR neighbor is in a stale state:

```
device# show ipv6 bgp summary

  BGP4 Summary
   Router ID: 140.1.1.3   Local AS Number: 50
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 4, UP: 1
  Number of Routes Installed: 13, Uses 1235 bytes
  Number of Routes Advertising to All Neighbors: 32 (16 entries), Uses 960 bytes
  Number of Attribute Entries Installed: 3, Uses 276 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  10.10.10.1        50          ACTIVs    0h 0m 0s    10       0        3        0 <
```

The following is sample output from the **show ipv6 bgp summary** command when a GR neighbor is in a restarting state:

```
device# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 140.1.1.3   Local AS Number: 50
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 4, UP: 1
  Number of Routes Installed: 13, Uses 1235 bytes
  Number of Routes Advertising to All Neighbors: 32 (16 entries), Uses 960 bytes
  Number of Attribute Entries Installed: 3, Uses 276 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  10.10.10.1        50          OPENSr    0h 0m 2s    10       0        0        3 <
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 counters interface

Displays the counters on an IPv6 interface.

Syntax

show ipv6 counters interface { <*N*>**gigabitethernet** *rbridge-id/slot/port* | **loopback** *port_number* | **ve** *vlan_id* }

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback *port_number*

Specifies the port number for the loopback interface. The range is 1 through 255.

ve *vlan_id*

Specifies the VLAN ID of a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Examples

The following example shows counters on an Ethernet interface:

```
switch# show ipv6 counters interface te 1/0/10
 Interface TenGigabitEthernet 1/0/10 IPv6 statistics (ifindex 402980872)
     Ip6OutRequests                          21
     Ip6OutMcastPkts                         30
     Ip6OutOctets                            2024
     Ip6OutMcastOctets                       3008
     Icmp6OutMsgs                            21
     Icmp6OutRouterAdvertisements            6
     Icmp6OutNeighborSolicits                6
     Icmp6OutMLDv2Reports                    9
     Icmp6OutType134                         6
     Icmp6OutType135                         6
     Icmp6OutType143                         25
```

show ipv6 dhcp relay address interface

Displays IPv6 DHCP Relay addresses configured on a specific interface.

Syntax

show ipv6 dhcp relay address interface [*interface-type interface-name*]{ **rbridge-id** *rbridge-id* | **all** | *range* }

Command Default

If the **rbridge-id** parameter is omitted, IPv6 DHCP Relay addresses display for the local switch.

Parameters

interface-type
Specifies the type of interface, such as gigabitEthernet, TengigabitEthernet, FortygigabitEthernet, HundredgigabitEthernet, or Ve interface.

interface-name
Specifies the interface number or VLAN-ID in case of a Ve interface.

rbridge-id *rbridge-id*
Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all
Specifies all RBridge IDs in the logical chassis cluster.

range
A range of RBridge IDs separated by a dashes or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

This command displays IPv6 DHCP Relay addresses configured on specific physical or virtual Ethernet (VE) interfaces located on a local switch, specific switches, or all switches in a logical chassis cluster. No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5).

Examples

Display configured IPv6 DHCP Relay addresses on a specific physical interface:

```
sw0# show ipv6 dhcp relay address interface tengigabitethernet 1/0/24
                                Rbridge Id: 3
                                ----------------
Interface                                Relay Address                              VRF
Name                 Outgoing Interface
-------------                -------------                                ---------
-------------------

Te 3/0/21                              4001::10                                default-
vrf
Te 3/0/21                              fe80::8
blue                       ve 100
```

Display configured IPv6 DHCP Relay addresses on VE interface for RBridge ID 1.

```
sw0# show ipv6 dhcp relay address int ve 300 rbridge-id 1
                                  Rbridge Id:    1
                                  ----------------
Interface              Relay Address                                        VRF Name
------------           --------------                                     --------
Ve 300                         5001:1234:1234:2101:1234:1234:3103:1234               default-vrf
```

Display configured IPv6 DHCP Relay addresses on VE interface on RBridge IDs 1 and 3.

```
sw0# show ipv6 dhcp relay address interface ve 300 rbridge-id 1,3
                                  Rbridge Id:    1
                                  ----------------
Interface                Relay Address                                                 VRF Name
---------                -------------                                                 --------
Ve 300                                5001:1234:1234:2101:1234:1234:3103:1234
default-vrf
                                  Rbridge Id:    3
                                  ----------------
Ve 300                                10.0.0.5                              default-vrf
```

History

Release version	Command history
5.0.1	This command was introduced.

show ipv6 dhcp relay address rbridge-id

Displays IPv6 DHCP Relay addresses.

Syntax

show ipv6 dhcp relay address rbridge-id *rbridge-id* | **all** | *range*

Command Default

If the *rbridge-id* parameter is omitted, IP DHCP Relay addresses display for the local switch.

Parameters

rbridge-id

Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all

Specifies all RBridge IDs in the logical chassis cluster.

range

A range of RBridge IDs separated by a dashes or commas, or both. Range can be discontiguous, for example, 1-3,5. Spaces are not allowed.

For example: 1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6. in the range string

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the IPv6 address and Virtual Routing and Forwarding (VRF) name for all interfaces with configured IPv6 DHCP Relay addresses on a local switch, specific switches, or all switches in a VCS Fabric cluster. No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5).

Examples

To display addresses configured on a specific RBridge ID:

```
sw0# show ipv6 dhcp relay address
                                Rbridge Id:    3
                                 ----------------
Interface              Relay Address                      VRF Name          Outgoing Interface
---------              -------------                    -------------
-----------------------
Te 3/0/21              4001::101                              default-vrf
Te 3/0/21              fe80::8                                blue                    ve 100
Ve 200                 5001:1234:1234:2101:1234:1234:3103:1234 default-vrf             Te 3/0/3
```

To display addresses configured on all switches in a virtual fabric cluster:

```
sw0# show ipv6 dhcp rel address rbridge-id all
                                Rbridge Id:    1
                                -------------
Interface                                Relay Address                                VRF Name
---------                                -------------                                --------
Te 1/0/24                                2.3.4.5                                      default-vrf
Ve 300                                   10.0.1.2                                     default-vrf
                                Rbridge Id:    3
                                -------------
Interface                                Relay Address                                VRF Name
---------                                -------------                                --------
Ve 300                                   10.0.0.5                                     default-vrf
```

History

Release version	Command history
5.0.1	This command was introduced.

show ipv6 dhcp relay statistics

Displays general information about the DHCPv6 Relay function.

Syntax

show ipv6 dhcp relay statistics rbridge-id *rbridge-id* | **all** | *range*]

Command Default

If the **rbridge-id** parameter is omitted, IPv6 DHCP Relay statistics display for the local switch.

Parameters

rbridge-id *rbridge-id*

Specifies an RBridge. You can specify multiple RBridge IDs, separated by commas.

all

Specifies all RBridge IDs in the logical chassis cluster.

range

A range of RBridge IDs separated by a dashes or commas, for example:

1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Modes

Privileged EXEC mode

Usage Guidelines

No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster. To display addresses for configured interfaces on a local switch, an RBridge ID parameter is not required.

The **show ipv6 dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on a local switch, specific switches, or all switches in a logical chassis cluster:

- Number of DHCP Error packets dropped.
- Number of DHCP SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, INFORMATION-REQUEST, RELAY-FORWARD, RELAY-REPLY packets received.
- Number of DHCP RELAY-FORWARD, REPLY packets sent.

Examples

To display statistics for a local switch:

```
sw0# show ipv6 dhcp relay statistics

Packets dropped               :  0
    Error                          :  0
Packets received              :  0
    SOLICIT                    :  0
    REQUEST                 :  0
    CONFIRM                  :  0
    RENEW                     :  0
    REBIND                     :  0
    RELEASE                  :  0
    DECLINE                   :  0
    INFORMATION-REQUEST       :  0
    RELAY-FORWARD        :  0
    RELAY-REPLY               :  0
Packets sent                  :  0
    RELAY-FORWARD   :  0
    REPLY                        :  0
```

To display statistics for specific RBridge IDs:

```
switch# show ipv6 dhcp relay statistics rbridge-id 6

                              Rbridge Id:    6
Packets dropped          : 0
  Error                  : 0
Packets received         : 6
  SOLICIT                : 2
  REQUEST                : 1
  CONFIRM                : 0
  RENEW                  : 0
  REBIND                 : 0
  RELEASE                : 0
  DECLINE                : 0
  INFORMATION-REQUEST    : 0
  RELAY-FORWARD          : 0
  RELAY-REPLY            : 3
Packets sent             : 6
  RELAY-FORWARD          : 3
  REPLY                  : 3
```

History

Release version	Command history
5.0.1	This command was introduced.

show ipv6 interface

Displays details of IPv6 interfaces.

Syntax

show ipv6 interface [**brief** [**rbridge-id** { **all** | *rbridge-id* }] | { *<N>***gigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* [**rbridge-id** { **all** | *rbridge-id* }] }

Parameters

brief

Specifies brief interface information.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace **<N>gigabitethernet** with the desired operand (for example, tengigabitethernet specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

ve *vlan_id*

Specifies the VLAN ID of a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Interface subtype configuration mode

Examples

The following example illustrates the output of the **show ipv6 interface** command with an Ethernet interface specified:

```
switch# show ipv6 interface tengigabitethernet 1/0/10
 TenGigabitEthernet 1/0/10 is up protocol is up
 IPv6 Address: 1111::2222/64  Primary  Confirmed
 IPv6 Address: fe80::227:f8ff:fe88:e4df/128  Link Local  Confirmed
 IPv6 MTU: 1500
 Vrf : default-vrf
```

The following example illustrates the output of the **show ipv6 interface** command with a virtual Ethernet and RBridge ID specified:

```
switch# show ipv6 interface ve 10 rbridge 1

 Ve 10 is administratively down protocol is down
 IPv6 Address: fe80::/128  Link Local  Wait Confirm
 IPv6 MTU: 1500
 Vrf : default-vrf
```

The following example illustrates the output of the **show ipv6 interface** command with a virtual Ethernet of 1 specified:

```
switch# #show ipv6 interface ve 1
 Ve 1 is up protocol is up
 IPv6 Address: 1001::4/64  Primary  Confirmed
 IPv6 Address: fe80::205:33ff:fee4:4011/128  Link Local  Confirmed
 IPv6 Address: fe80::205:33ff:fee5:ba86/128  Link Local  Confirmed
 IPv6 multicast groups locally joined:
    ff02::1
    ff02::2    ff02::1:ff00:4    ff02::1:ffe4:4011
    ff02::1:ffe5:ba86
 IPv6 MTU: 1500
 Vrf : default-vrf
```

The following example illustrates the output of the **show ipv6 interface** applied directly on an interface with the **brief** option:

```
switch(conf-if-te-1/0/10)# do show ipv6 int br
Interface      Vrf                    Status        Protocol         IPv6-Address
================================================================================
FortyGigabitEthernet 1/0/49       default-vrf             up            up           unassigned
FortyGigabitEthernet 1/0/50       default-vrf             up            down         unassigned
FortyGigabitEthernet 1/0/51       default-vrf             up            down         unassigned
FortyGigabitEthernet 1/0/52       default-vrf             up            down         unassigned
TenGigabitEthernet 1/0/1          default-vrf             up            down         unassigned
TenGigabitEthernet 1/0/2          default-vrf             up            down         unassigned
TenGigabitEthernet 1/0/10         default-vrf             up            up           1111::2222/64
```

show ipv6 mld groups

Displays information about a specific IPv6 MLDv1 group or a VLAN.

Syntax

show ipv6 mld groups [*ipv6address*] [**interface vlan** *vlan_id*]

Parameters

ipv6address
A multicast group address.

interface vlan
Specifies a VLAN ID.

vlan_id
A VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

Modes

Privileged EXEC mode

Examples

To display information about all IPv6 MLDv1 groups:

```
switch# show ipv6 mld groups
```

To display information about an IPv6 MLDv1 group for a specific multicast address:

```
switch# show ipv6 mld groups ff1e::1
```

To display information about all IPv6 MLDv1 groups for a VLAN:

```
switch# show ipv6 mld groups interface vlan 2000
```

show ipv6 mld interface

Displays IPv6 MLDv1 snooping information for a VLAN interface.

Syntax

show ipv6 mld interface { **vlan** *vlan_id* } [**rbridge-id** { **all** | *rbridge-id* }]

Parameters

vlan *vlan_id*

Specifies a VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

To display information about IPv6 MLDv1 snooping for a specific VLAN interface:

```
switch# show ipv6 mld statistics interface vlan 1
MLD packet statistics for Rbridge Id 3 in Vlan vlan1
MLD Message type      Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL-Received
General Query               0            0             0              0 <<
Group Specific Query        0            0             0              0
V1 Membership Report        0            0             0              0
V2 Membership Report        0            0             0              0
Group Leave                 0            0             0              0

MLD Error Statistics:
Checksum Error              0
Size_or_Range_Error         0
```

show ipv6 mld snooping

Displays information about the actively enabled IPv6 MLDv1 snooping mechanism and related configurations such as the active querier, the number of group-learned mrouters present, and other querier details.

Syntax

show ipv6 mld snooping [**interface vlan** *vlan_id*] [**mrouter** [**interface vlan** *vlan_id*]]

Parameters

interface vlan

Specifies a VLAN ID.

vlan_id

A VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

mrouter

Specifies all multicast router statistics.

Modes

Privileged EXEC mode

Examples

To display comprehensive information about the IPv6 MLDv1 snooping mechanism and related configurations:

```
switch# show ipv6 mld snooping
```

To display information about IPv6 MLDv1 snooping for a specific VLAN:

```
switch# show ipv6 mld snooping interface vlan 2000
```

To display information about all IPv6 MLDv1 multicast router snooping:

```
switch# show ipv6 mld snooping mrouter
```

To display information about IPv6 MLDv1 multicast router snooping for a specific VLAN:

```
switch# show ipv6 mld snooping mrouter interface vlan 2000
```

show ipv6 mld statistics

Displays IPv6 MLDv1 statistics for a VLAN.

Syntax

show ipv6 mld statistics interface vlan *vlan_id* [**rbridge-id** { **all** | *rbridge-id* }]

Parameters

interface vlan

Specifies a VLAN ID.

vlan_id

A VLAN ID. Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

To display information about IPv6 MLDv1 snooping statistics for a specific VLAN:

```
switch# show ipv6 mld statistics interface vlan 2000
```

show ipv6 nd interface

Displays information about the IPv6 Neighbor Discovery configuration on an interface.

Syntax

show ipv6 nd interface [*<N>*__gigabitethernet__ *rbridge-id/slot/port* | **prefix** | **rbridge-id** { **all** | *rbridge-id* } | **ve** *vlan_id* [**prefix**] | **vrf** { *vrf-name* | **all** | **default**]]

Parameters

*<N>*__gigabitethernet__

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>*__gigabitethernet__ with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

prefix

Displays prefix information.

rbridge-id

Specifies the RBridge IDs. You can display all or a specific RBridge.

all

Specifies all RBridges in the cluster.

rbridge-id

Specifies a single RBridges in the cluster.

ve *vlan_id*

Specifies the VLAN ID of a virtual Ethernet (VE) interface.

vrf *vrf-name*

Specifies a VRF instance.

all

Specifies all VRF instances.

default

Specifies the default VRF instance.

Modes

Privileged EXEC mode

Examples

The following example illustrates the output of the **show ipv6 nd interface** command for an Ethernet interface:

```
switch# show ipv6 nd interface tengigabitethernet 7/0/46
ICMPv6 ND Interfaces for VRF  default-vrf
  IPv6 address:  2ffe::1
  Router-Advertisement active timers:
    Last Router-Advertisement sent: 00:01:25
    Next Router-Advertisement sent in: 00:07:06
  Router-Advertisement parameters:
    Periodic interval:  200 to 600 seconds
    Send 'Managed Address Configuration' flag: false
    Send 'Other Stateful Configuration' flag: false
    Send 'Current Hop Limit' field: 64
    Send 'MTU' option value: 1500
    Send 'Router Lifetime' field: 1800 secs
    Send 'Reachable Time' field: 0 ms
    Send 'Retrans Timer' field: 0 ms
    Suppress RA: false
    Suppress MTU in RA: false
    Suppress All RA: false
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1 secs
    DAD Attempts: 2
    DAD expiry: 1 secs
  Neighbor Cache Expiry: 240 mins
```

The following example illustrates the output of the **show ipv6 nd interface** command for an Ethernet interface with the **prefix** keyword specified:

```
switch# show ipv6 nd interface tengigabitethernet 7/0/46 prefix
ICMPv6 ND Interfaces for VRF  default-vrf
 List of IPv6 Prefix advertised on  Te 7/0/46
     Prefix :  3001::/64
     Enabled :  Yes
     Valid lifetime :  2592000
     Preferred lifetime :  604800
     On-link :  Yes
     Off-link :  No
     Autonomous :  Yes
     Prefix :  2ffe::/64
     Enabled :  Yes
     Valid lifetime :  Infinite
     Preferred lifetime :  Infinite
     On-link :  Yes
     Off-link :  No
     Autonomous :  Yes
```

show ipv6 neighbor

Displays information for a neighbor in IPv6 Neighbor Discovery.

Syntax

show ipv6 neighbor [*<N>* **gigabitethernet** [**dynamic** | **summary**][**vrf** [*vrf-name* | **all** | **default-vrf**]] [**rbridge-id** { **all** | *rbridge-id* } | **slot** *slot* [*ipv6_address*]] | **static** [**summary** [**vrf** [*vrf-name* | **all** | **default-vrf**]] | **ve** *vlan_id*]

Parameters

dynamic

Displays dynamic information.

summary

Displays summary information.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

vrf *vrf-name*

Specifies a VRF instance.

all

Specifies all VRF instances.

default-vrf

Specifies the default VRF instance.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

all

Specifies all RBridges in the cluster.

slot *slot*

Specifies a line card.

static

Displays static information.

ve *vlan_id*

Specifies the VLAN ID of a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Examples

The following example illustrates the output of the **show ipv6 neighbor** command without keywords:

```
switch# show ipv6 neighbor
Address         Mac-address    Interface     MacResolved   Age         Type
-------------------------------------------------------------------------------
2001::10    0010.9400.0066  Te 3/0/2     yes           00:00:13    Dynamic
2001::11    0010.9400.0067  Te 3/0/2     yes           00:00:13    Dynamic
2001::12    0010.9400.0068  Te 3/0/2     yes           00:00:13    Dynamic
2001::13    0010.9400.0069  Te 3/0/2     yes           00:00:13    Dynamic
2001::14    0010.9400.006a  Te 3/0/2     yes           00:00:13    Dynamic
2001::15    0010.9400.006b  Te 3/0/2     yes           00:00:13    Dynamic
2001::16    0010.9400.006c  Te 3/0/2     yes           00:00:13    Dynamic
2001::17    0010.9400.006d  Te 3/0/2     yes           00:00:13    Dynamic
2001::18    0010.9400.006e  Te 3/0/2     yes           00:00:13    Dynamic
```

The following example illustrates the output of the **show ipv6 neighbor** command with the `slot` keyword:

```
switch# show ipv6 neighbor slot 0
Total Neighbors : 100
Address     Mac-address     Interface     MacResolved   Type
-------------------------------------------------------------------------------
2001::10    0010.9400.0066  Te 0/2        yes           Dynamic
2001::11    0010.9400.0067  Te 0/2        yes           Dynamic
2001::12    0010.9400.0068  Te 0/2        yes           Dynamic
2001::13    0010.9400.0069  Te 0/2        yes           Dynamic
```

show ipv6 ospf area

Displays the OSPFv3 area table in a specified format.

Syntax

show ipv6 ospf area [*A.B.C.D*] [*decimal*] [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format. Valid values range from 0 to 2147483647.

all-vrfs

Specifies all VRFs.

rbridge-id *rbridge-id*

Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf area** command when no arguments or keywords are used:

```
switch# show ipv6 ospf area
Area 0.0.0.1 :
Authentication: Not Configured
Active interface(s)attached to this area: Ve 2001 Ve 2002
Inactive interface(s)attached to this area: None
Number of Area scoped LSAs is 38
Sum of Area LSAs Checksum is 0015da81
Statistics of Area 0.0.0.1:
SPF algorithm executed 46 times
SPF last updated: 8518 sec ago
Current SPF node count: 7
Router: 4 Network: 3
Maximum of Hop count to nodes: 4
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf database

Displays lists of information about different OSPFv3 link-state advertisements (LSAs).

Syntax

show ipv6 ospf database [**advrtr** *A.B.C.D*] [**all-vrfs**] [**as-external**] [**extensive**] [**inter-prefix**] [**inter-router**] [**intra-prefix**] [**link** *decimal*] [**link-id** *decimal*] [**network**] [**prefix** *ipv6-addr*] [**rbridge-id** *rbridge-id*] [**router**] [**summary**] [**type-7**] [**vrf** *vrfname*]

show ipv6 ospf database scope { **area** { *A.B.C.D* | *decimal* } | **as** | **link** } [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

advrtr *A.B.C.D*
Displays LSAs by Advertising Router Id in dotted decimal format.

all-vrfs
Specifies all VRFs in the cluster.

as-external
Displays information about external LSAs.

extensive
Displays detailed lists of LSA information.

inter-prefix
Displays information about inter area prefix LSAs.

inter-router
Displays information about inter area router LSAs.

intra-prefix
Displays information about intra area router LSAs.

link *decimal*
Displays information about the link LSAs.

link-id *decimal*
Link-state ID that differentiates LSAs. Valid values range from 1 to 4294967295.

network
Displays information about the network LSAs.

prefix
Displays information on the intra-area-prefix LSAs.

ipv6-addr
IPv6 address in dotted-decimal notation.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

router
Displays information about the router LSAs.

summary
Displays LSA summary information.

type-7
Displays information about the not so stubby area (NSSA) external LSAs.

vrf vrf *name*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

scope
Displays LSA information by LSA scope.

area
Displays LSAs by scope within a specified area.

as
Displays autonomous system (AS) LSAs by scope.

link
Displays link LSAs by scope.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf database as-external** command using the **link-id** keyword:

```
device# show ipv6 ospf database as-external link-id 5
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
N/A             Extn 33         4.4.4.4         80000002 1044 acb8  36    Yes
Bits: E--
Metric: 0
     Prefix Options:
     Referenced LSType: 0
     Prefix: 2001:2:16::/64
```

The following is sample output from the **show ipv6 ospf database inter-prefix** command using the **link-id** keyword:

```
device# show ipv6 ospf database inter-prefix link-id 5
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
128             Inap 5          125.125.125.125 80000035 548  fe72  36    Yes
     Metric: 1
     Prefix Options:
     Prefix: 2001:2000:8192::/64
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
128             Inap 5          122.122.122.122 80000035 565  a7e8  36    Yes
     Metric: 1
     Prefix Options:
     Prefix: 2001:2001::/64
```

The following is sample output from the **show ipv6 ospf database inter-router** command using the **link-id** keyword:

```
device# show ipv6 ospf database inter-router link-id 5
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0.0.0.0         Inar 5          125.125.125.125 80000035 879  c910  32    Yes
     Options: V6E---R--
     Metric: 1
     Destination Router ID: 125.2.32.125
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0.0.0.1         Inar 5          122.122.122.122 80000035 1611 bb3c  32    Yes
     Options: ---------
     Metric: 2
     Destination Router ID: 125.2.32.125
```

The following is sample output from the **show ipv6 ospf database intra-prefix** command using the **link-id** keyword:

```
device# show ipv6 ospf database intra-prefix link-id 5
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Iap  0          10.10.10.10     80000002 1572 63a0  44    Yes
     Number of Prefix: 1
     Referenced LS Type: Router
     Referenced LS ID: 0
     Referenced Advertising Router: 10.10.10.10
     Prefix Options:  Metric: 1
     Prefix: 2050::/64
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Iap  46440      4.4.4.4         80000001 1649 d85c  44    Yes
     Number of Prefix: 1
     Referenced LS Type: Network
     Referenced LS ID: 1548
     Referenced Advertising Router: 4.4.4.4
     Prefix Options:  Metric: 0
     Prefix: 3010::/64
```

The following is sample output from the **show ipv6 ospf database link** command using the **link-id** keyword:

```
device# show ipv6 ospf database link link-id 5
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Link 145        10.10.10.10     80000001 1639 0117  56    Yes
     Router Priority: 1
     Options: V6E---R--
     LinkLocal Address: fe80::205:33ff:fe77:2452
     Number of Prefix: 1
     Prefix Options:
     Prefix: 2050::/64
```

The following is sample output from the **show ipv6 ospf database network** command:

```
device# show ipv6 ospf database network
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Net  1548       4.4.4.4         80000001 1707 7b53  32    Yes
     Options: V6E---R--
     Attached Router: 4.4.4.4
     Attached Router: 10.10.10.10
```

The following is sample output from the **show ipv6 ospf database router** command:

```
device# show ipv6 ospf database router
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Rtr  0          4.4.4.4         80000139 2    4b9a  24    Yes
  Capability Bits: ---EB
  Options: V6E---R--
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
10              Rtr  0          4.4.4.4         80000001 2    e236  24    Yes
  Capability Bits: ---EB
        Options: V6---NR--
```

The following is sample output from the **show ipv6 ospf database type-7** command:

```
device# show ipv6 ospf database type-7
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
3               Typ7 3          10.10.10.10     80000001 5    6c95  28    Yes
     Bits: E--
     Metric: 10
     Prefix Options:
     Referenced LSType: 0
     Prefix: ::/0
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
3               Typ7 2          10.10.10.10     80000001 5    8107  36    Yes
     Bits: E--
     Metric: 10
     Prefix Options:
     Referenced LSType: 0
                    Prefix: 2111::/64
```

The following is sample output from the **show ipv6 ospf database link-id** command:

```
device# show ipv6 ospf database link-id 6514
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Link 6514       10.10.10.10     80000001 1696 6e44  56    Yes
     Router Priority: 1
     Options: V6E---R--
     LinkLocal Address: fe80::205:33ff:fe77:23ee
     Number of Prefix: 1
     Prefix Options:
     Prefix: 3010::/64
```

The following is sample output from the **show ipv6 ospf database extensive** command:

```
device# show ipv6 ospf database extensive
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Link 145        10.10.10.10     80000001 1559 0117  56    Yes
     Router Priority: 1
     Options: V6E---R--
     LinkLocal Address: fe80::205:33ff:fe77:2452
     Number of Prefix: 1
     Prefix Options:
     Prefix: 2050::/64
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Link 6514       10.10.10.10     80000001 1592 6e44  56    Yes
                    Router Priority: 1
                    Options: V6E---R--
                    LinkLocal Address: fe80::205:33ff:fe77:23ee
                    Number of Prefix: 1
                    Prefix Options:
                    Prefix: 3010::/64
```

The following is sample output from the **show ipv6 ospf database summary** command:

```
device# show ipv6 ospf database summary
AS scope:
                      Active     MaxAge
 ASExternal                6          0
Area 0 scope:
                      Active     MaxAge
 Router                    2          0
 Network                   1          0
 InterPrefix               1          0
 InterRouter               0          0
 Type7                     0          0
 IntraPrefix               2          0
 Other                     0          0
 Total                     6          0
 Interface scope (over 2 interfaces):
                       Active     MaxAge
  Link                      3          0
  Grace                     0          0
  Other                     0          0
  Total                     3          0
Area 1 scope:
                      Active     MaxAge
Router                    1          0
 Network                  0          0
 InterPrefix              2          0
 InterRouter              1          0
 Type7                    0          0
 IntraPrefix              1          0
 Other                    0          0
 Total                    5          0
 Interface scope (over 1 interfaces):
                       Active     MaxAge
  Link                     1          0
  Grace                    0          0
  Other                    0          0
  Total                    1          0
Total: 21 LSAs, 21 Active LSAs, 0 MaxAge LSAs
```

The following is sample output from the **show ipv6 ospf database scope** command using the **area** keyword:

```
device# show ipv6 ospf database scope area 0
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Rtr  0          10.10.10.10     80000005 1135 4bf6  40    Yes
  Capability Bits: ---EB
  Options: V6E---R--
  Type: Transit Metric: 1
  Interface ID: 6514        Neighbor Interface ID: 1548
  Neighbor Router ID: 4.4.4.4
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Rtr  0          4.4.4.4         800000f1 1295 9156  40    Yes
  Capability Bits: ---E-
  Options: V6E---R--
  Type: Transit Metric: 1
  Interface ID: 1548        Neighbor Interface ID: 1548
  Neighbor Router ID: 4.4.4.4
```

The following is sample output from the **show ipv6 ospf database prefix** command:

```
device# show ipv6 ospf database prefix L5001::10/128
LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace
Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Iap  0          4.4.4.4         80000001 267  52a8  52    Yes
     Number of Prefix: 1
     Referenced LS Type: Router
     Referenced LS ID: 0
     Referenced Advertising Router: 4.4.4.4
     Prefix Options: LA, Metric: 0
     Prefix: 5001::10/128
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax

show ipv6 ospf interface [**all-vrfs**] [**brief**] [*<N>***gigabitethernet** *mappedID/slot/port*] [**loopback** *number*] [**rbridge-id** *rbridge-id*] [**ve** *vlan_id*] [**vrf** *vrfname*]

Parameters

all-vrfs

Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopback or SVI interfaces with the same id from different rbridges. If *rbridge-id* is not specified the output will contain information from all vrfs from the local node only.

brief

Displays brief summary about all enabled interfaces.

*<N>***gigabitethernet** *rbridge-id/slot/port*

Specifies a valid, physical Ethernet subtype (*<N>* represents all available Ethernet speeds). Enter **?** at the command prompt to see what interface subtypes are available for that command.

rbridge-id

Specifies the RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid slot number.

ve *vlan_id*

Specifies the VLAN number.

rbridge-id

Specifies the RBridge ID.

loopback *number*

Specifies a loopback port number in the range from 1 through 255.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **brief** keyword to limit the display to the following fields:

- Interface

- Area
- Status
- Type
- Cost
- State
- Nbrs(F/C)

Examples

The following is sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used:

```
device# show ipv6 ospf interface
vlan0.10 admin up, oper up, IPv6 enabled
IPv6 Address:fe80::205:33ff:fe77:23ee
3010::10/64
Instance ID 0, Router ID 10.10.10.10
Area ID 0, Cost 1, Type BROADCAST
MTU: 1500
State BDR, Transmit Delay 1 sec, Priority 1, Link-LSA Tx not suppressed
Timer intervals :
Hello 10, Hello Jitter 10 Dead 40, Retransmit 5
Authentication Use: Enabled
KeyRolloverTime(sec): Configured: 300 Current: 0
KeyRolloverState: NotActive
Outbound: None
Inbound: None
DR:4.4.4.4 BDR:10.10.10.10 Number of I/F scoped LSAs is 2
DRElection: 1 times, DelayedLSAck: 2 times
Neighbor Count = 1, Adjacent Neighbor Count= 1
Neighbor:
4.4.4.4 (DR)
Statistics of interface vlan0.10:
Type tx rx tx-byte rx-byte
Unknown 0 0 0 0
Hello 37 35 1476 1400
DbDesc 2 2 136 116
LSReq 1 1 52 64
LSUpdate 8 2 684 368
LSAck 3 8 208 348
OSPF messages dropped,no authentication: 0
```

The following is sample output from the **show ipv6 ospf interface** command the **brief** keyword is used:

```
device# show ipv6 ospf interface brief
Interface Area Status Type Cost State Nbrs(F/C)
te2/1      0     up   BCST  1    DR    0/0
vlan0.10   0     up   BCST  1    BDR   1/1
vlan0.20   1     up   BCST  1    DR    0/0
vlan0.30   1     up   P2P   10   P2P   0/0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf memory

Displays information about OSPFv3 memory usage.

Syntax

show ipv6 ospf memory [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

all-vrfs
Displays the information for all VRF instances.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*
Displays the information for a specific VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display routes that have been redistributed into OSPFv3.

Examples

The following is sample output from the **show ipv6 ospf memory** command when no arguments or keywords are used:

```
device# show ipv6 ospf memory
Total Dynamic Memory Allocated for this instance : 4551924 bytes
Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_AREA          450720     2          4          0
   MTYPE_OSPF6_AREA_RANGE    36         0          16         0
   MTYPE_OSPF6_SUMMARY_ADDRE 32         0          16         0
   MTYPE_OSPF6_IF            304        4          64         0
   MTYPE_OSPF6_NEIGHBOR      12524      1          32         0
   MTYPE_OSPF6_ROUTE_NODE    28         11         4096       0
   MTYPE_OSPF6_ROUTE_INFO    44         11         4096       0
   MTYPE_OSPF6_PREFIX        24         0          16         0
   MTYPE_OSPF6_LSA           136        22         4096       0
   MTYPE_OSPF6_VERTEX        176        4          64         0
   MTYPE_OSPF6_SPFTREE       48         2          2          0
   MTYPE_OSPF6_NEXTHOP       32         7          256        0
   MTYPE_OSPF6_EXTERNAL_INFO 44         0          4096       0
   MTYPE_THREAD              36         13         1024       0
   MTYPE_OSPF6_LINK_LIST     24         3224       20480      0
   MTYPE_OSPF6_LINK_NODE     16         74         20480      0
   MTYPE_OSPF6_LSA_RETRANSMI 12         0          8192       0
   global memory pool for all instances
   Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_TOP           61480      1          1          0
   MTYPE_OSPF6_LSA_HDR       56         22         23         0
   MTYPE_OSPF6_RMAP_COMPILED 0          0          0          0
   MTYPE_OSPF6_OTHER         0          0          0          0
   MTYPE_THREAD_MASTER       84         1          1          0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf neighbor

Displays detailed or summary OSPFv3 neighbor information.

Syntax

show ipv6 ospf neighbor [**all-vrfs**] [**detail**] [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **ve** *vlan_id* }] [**rbridge-id** *rbridge-id*] [**router-id** *A.B.C.D*] [**vrf** *vrfname*]

Parameters

all-vrfs
Displays the information for all VRF instances.

detail
Displays detailed neighbor information.

Interface
Displays OSPFv3 interface information.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

loopback *number*
Specifies a loopback port number in the range from1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

router-id *A.B.C.D*
Displays neighbor information for the specified router ID (in dotted decimal format).

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf neighbor** command when no arguments or keywords are used:

```
device# show ipv6 ospf neighbor
Total number of neighbors in all states: 1
Number of neighbors in state Full      : 1
RouterID        Pri State    DR              BDR             Interface     [State]
4.4.4.4           1 Full     4.4.4.4         10.10.10.10     vlan0.10      [BDR]
```

The following is sample output from the **show ipv6 ospf neighbor** command when the **detail** keyword is used:

```
device# show ipv6 ospf neighbor detail
Total number of neighbors in all states: 8
Number of neighbors in state Init      : 1
Number of neighbors in state Full      : 7
RouterID        Pri State    DR              BDR             Interface     [State]
153.153.153.153   1 Init     153.153.153.153 0.0.0.0         Fo 122/8/8    [DR]
                Option: 00-00-00    QCount: 0    Timer: 37
125.125.125.125   1 Full     154.154.154.154 122.122.122.122 Ve 2000       [BDR]
                Option: 00-00-13    QCount: 0    Timer: 2
154.154.154.154   1 Full     154.154.154.154 122.122.122.122 Ve 2000       [BDR]
                Option: 00-00-13    QCount: 0    Timer: 38
122.21.21.122     0 Full     122.122.122.122 0.0.0.0         Ve 2001       [DR]
                Option: 00-00-13    QCount: 0    Timer: 18
125.125.125.125   1 Full     122.122.122.122 125.125.125.125 Ve 2002       [DR]
                Option: 00-00-13    QCount: 0    Timer: 5
125.125.125.125   1 Full     122.122.122.122 125.125.125.125 Ve 2009       [DR]
                Option: 00-00-13    QCount: 0    Timer: 47
125.125.125.125   1 Full     128.128.128.128 125.125.125.125 Ve 2128       [DROt her]
                Option: 00-00-13    QCount: 42    Timer: 420
128.128.128.128   1 Full     128.128.128.128 125.125.125.125 Ve 2128       [DROt her]
                Option: 00-00-13    QCount: 0    Timer: 28
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf redistribute route

Displays all IPv6 routes or a specified IPv6 route that the device has redistributed into OSPFv3.

Syntax

show ipv6 ospf redistribute route [*A.B.C.D:M*] [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

A.B.C.D:M
Specifies an IPv6 address.

all-vrfs
Displays all IPv6 routes that the device has redistributed into OSPFv3.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf redistribute route** command when no arguments or keywords are used:

```
device# show ipv6 ospf redistribute route
Id      Prefix          Protocol  Metric Type  Metric
2       2111::/64       Static    Type-2       10
1       3030::/64       Connect   Type-2       0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf routes

Displays OSPFv3 routes.

Syntax

show ipv6 ospf routes [*A.B.C.D:M*] [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

A.B.C.D:M

Specifies a destination IPv6 address.

all-vrfs

Displays the entire OSPFv3 route table for a device.

rbridge-id *rbridge-id*

Displays the route information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

To display OSPFv3-calculated routes for the default VRF:

```
device# show ipv6 ospf routes

Current Route count: 4
    Intra: 3 Inter: 0 External: 5 (Type1 0/Type2 5)
    Equal-cost multi-path: 0
    OSPF Type: IA- Intra, OA - Inter, E1 - External Type1, E2 - External Type2
   Destination                    Cost       E2Cost     Tag        Flags    Dis
E2 2014::/64                      1          0          0          00000003 110
   Next_Hop_Router                Outgoing_Interface Adv_Router
   fe80::768e:f8ff:fe2a:4900      vlan0.10           4.4.4.4
   Destination                    Cost       E2Cost     Tag        Flags    Dis
E2 2015::/64                      1          0          0          00000003 110
   Next_Hop_Router                Outgoing_Interface Adv_Router
   fe80::768e:f8ff:fe2a:4900      vlan0.10           4.4.4.4
   Destination                    Cost       E2Cost     Tag        Flags    Dis
IA 2050::/64                      1          0          0          00000003 110
   Next_Hop_Router                Outgoing_Interface Adv_Router
   ::                             te2/1              10.10.10.10
   Destination                    Cost       E2Cost     Tag        Flags    Dis
IA 3010::/64                      1          0          0          00000003 110
   Next_Hop_Router                Outgoing_Interface Adv_Router
   ::                             vlan0.10           4.4.4.4
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf spf

Displays OSPFv3 SPF node, table, and tree information.

Syntax

show ipv6 ospf spf { **node** | **table** | **tree** } [**all-vrfs**] [**area** { *A.B.C.D* | *decimal* }] | [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

node
Displays OSPFv3 node information.

table
Specifies a SPF table.

tree
Specifies a SPF tree.

all-vrfs
Displays the information for all VRF instances.

area
Specifies an area.

A.B.C.D
Area address in dotted decimal format.

decimal
Area address in decimal format.

rbridge-id *rbridge-id*
Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*
Displays the information for a specific VRF instance. If this option is not used, details for the default VRF are shown in the output.

Examples

The following is sample output from the **show ipv6 ospf spf** command when the **node** keyword is used:

```
device# show ipv6 ospf spf node
SPF node for Area 0
 SPF node 10.10.10.10,  cost: 0,  hops: 0
  nexthops to node:
  parent nodes:
  child nodes: 4.4.4.4:1548
 SPF node 4.4.4.4:1548,  cost: 1,  hops: 1
  nexthops to node:    :: vlan0.10
  parent nodes: 10.10.10.10
  child nodes: 4.4.4.4:0
 SPF node 4.4.4.4:0,  cost: 1,  hops: 2
  nexthops to node:    fe80::768e:f8ff:fe2a:4900 vlan0.10
  parent nodes: 4.4.4.4:1548
  child nodes:
SPF node for Area 1
 SPF node 10.10.10.10,  cost: 0,  hops: 0
  nexthops to node:
  parent nodes:
        child nodes:
```

The following is sample output from the **show ipv6 ospf spf** command when the **table** keyword is used:

```
device# show ipv6 ospf spf table
SPF table for Area 0
R 4.4.4.4              ---E- V6E---R--    1  fe80::768e:f8ff:fe2a:4900 vlan0.10
N 4.4.4.4[1548]        ----- V6E---R--    1  ::                         vlan0.10
  Destination           Bits Options  Cost  Nexthop                   Interface
 SPF table for Area 1
  Destination           Bits Options  Cost  Nexthop                   Interface
```

The following is sample output from the **show ipv6 ospf spf** command when the **tree** keyword is used:

```
device# show ipv6 ospf spf tree
SPF tree for Area 0
 +- 10.10.10.10 cost 0
     +- 4.4.4.4:1548 cost 1
         +- 4.4.4.4:0 cost 1

 SPF tree for Area 1
 +- 10.10.10.10 cost 0
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

Syntax

show ipv6 ospf summary [**all-vrfs**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

all-vrfs

Specifies all VRF instances.

rbridge-id *rbridge-id*

Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf summary** command when no arguments or keywords are used:

```
device# show ipv6 ospf summary

Total number of IPv6 OSPF instances: 1
Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     3       1       1         21      9
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf virtual-links

Displays information about all OSPFv3 virtual links or specified links.

Syntax

show ipv6 ospf virtual-link [**all-vrfs**] [**brief**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

all-vrfs
Specifies all virtual links.

brief
Displays brief summary information.

rbridge-id *rbridge-id*
Displays information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display brief or detailed information about virtual links. You can show information about all virtual links, or you can specify a virtual link

Use the **brief** keyword to limit the display to the following fields:

- Index
- Transit Area ID
- Router ID
- Interface Address
- State

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command when no arguments or keywords are used:

```
device# show ipv6 ospf virtual-links
Transit Area ID  Router ID        Interface Address             State
1                4.4.4.4          3010::10                      P2P
  Timer intervals(sec) :
    Hello 10, Hello Jitter 10,  Dead 40, Retransmit 5, TransmitDelay 1
  DelayedLSAck:     3 times
  Authentication: Not Configured
  Statistics:
      Type     tx          rx          tx-byte     rx-byte
      Unknown  0           0           0           0
      Hello    3           4           120         156
      DbDesc   2           3           156         124
      LSReq    1           1           40          76
      LSUpdate 7           3           656         240
      LSAck    3           4           148         224
      OSPF messages dropped,no authentication: 0
  Neighbor: State: Full Address: 3010::1 Interface: vlan0.10
```

The following is sample output from the **show ipv6 ospf virtual-links** command when the **brief** keyword is used:

```
device# show ipv6 ospf virtual-links brief
Transit Area ID  Router ID        Interface Address             State
1                4.4.4.4          3010::10                      P2P
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 ospf virtual-neighbor

Displays information about all OSPFv3 virtual neighbors or one OSPFv3 virtual neighbor that you specify.

Syntax

show ipv6 ospf virtual-neighbor [**all-vrfs**] [**brief**] [**rbridge-id** *rbridge-id*] [**vrf** *vrfname*]

Parameters

all-vrfs
Specifies all virtual neighbors.

brief
Displays brief summary information.

rbridge-id *rbridge-id*
Displays information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

vrf *vrfname*
Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display brief or detailed information about virtual neighbors. You can show information about all virtual neighbors, or you can specify a virtual neighbor

Use the **brief** keyword to limit the display to the following fields:

- Index
- Router ID
- Address
- State
- Interface

Examples

The following is sample output from the **show ipv6 ospf virtual-neighbor** command when no arguments or keywords are used:

```
device# show ipv6 ospf virtual-neighbor
Index Router ID        Address                     State     Interface
1     4.4.4.4          3010::1                     Full      vlan0.10
Option: 00-00-00    QCount: 0    Timer: 457
```

The following is sample output from the **show ipv6 ospf virtual-neighbor** command when the brief keyword is used:

```
device# show ipv6 ospf virtual-neighbor brief
Index Router ID        Address                      State     Interface
1     4.4.4.4          3010::1                      Full      vlan0.10
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 prefix-list

Displays the IPv6 prefix-list information.

Syntax

show ipv6 prefix-list [*name*]

Parameters

name

The name of the specific prefix-list you want to display.

Modes

Privileged EXEC mode

Examples

Typical command output:

```
switch# show ipv6 prefix-list
ipv6 prefix-list routesfor2001: 1 entries
seq 5 permit 2001::/16
```

Related Commands

ipv6 prefix-list

show ipv6 route

Displays information about IPv6 routes.

Syntax

show ipv6 route [*ipv6address* [**debug** [**rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** }] | **detail** [**rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** }] | **rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** } | *ipv6prefix* [**debug** | **detail** | **longer** [**rbridge-id** { **all** | *rbridge-id* }] **vrf** { *vrf-name* | **all** | **default** } | **all** [**rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** }] | **bgp** [**rbridge-id** *rbridge-id*] | **connected** [**rbridge-id** { **all** | *rbridge-id* }] **vrf** { *vrf-name* | **all** | **default** } | **nexthop** *nexthop* [**rbridge-id** { **all** | *rbridge-id* }] **vrf** { *vrf-name* | **all** | **default** } | **ospf** [**rbridge-id** *rbridge-id*] | **rbridge-id** { **all** | *rbridge-id* } | **slot** *slot* | **static** [**rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** } [**summary** [**rbridge-id** { **all** | *rbridge-id* } **vrf** { *vrf-name* | **all** | **default** }] [**vrf** [*vrf-name* | **all** | **default**]] | **vrf** [*vrf-name* | **all** | **default**]]

Parameters

ipv6address
IPv6 address in *A:B::C:D* format.

debug
Displays debug information.

detail
Displays detailed information.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

all
Specifies all RBridges in the cluster.

vrf *vrf-name*
Specifies a VRF instance.

all
Specifies all VRF instances.

default
Specifies the default VRF instance.

ipv6prefix
IPv6 prefix in *A:B::/length* format.

longer
Displays information for prefixes longer than the specified prefix.

all
Displays information about all routes.

bgp
Displays information about BGP routes.

connected
Displays information about directly connected routes.

nexthop *nexthop*
Displays information about a specified next-hop address.

slot *slot*
Specifies a line card.

static
Displays information about static routes.

summary
Displays summary information.

Modes

Privileged EXEC mode

show ipv6 route import

Displays the IPv6 routes imported to a specified VRF

Syntax

show ipv6 route import [**vrf** *vrf_name*] [**rbridge-id** {*rbridge-id* | **all**}]

Parameters

vrf_name

Specifies the VRF whose imported routes you want to display.

rbridge-id

Specifies a RBridge or all RBridges for the VRF whose routes you wish to display.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

To display IPv6 routes for a VRF that has been configured with the name VRF1:

```
switch# show ipv6 route import vrf vrf1
IPv6 Routing Table for VRF "vrf1"
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]

5000::/64, attached
    *via 2000:21::200, Ve 21, [20/0], 1m6s, eBgp+
5000:0:0:1::/64, attached
    *via 2000:21::200, Ve 21, [20/0], 1m6s, eBgp+
5000:0:0:2::/64, attached
    *via 2000:22::200, Ve 22, [20/0], 1m6s, eBgp+
5000:0:0:3::/64, attached
    *via 2000:22::200, Ve 22, [20/0], 1m6s, eBgp+
5000:0:0:4::/64, attached
    *via 2000:23::200, Ve 23, [20/0], 1m6s, eBgp+
5000:0:0:5::/64, attached
    *via 2000:24::200, Ve 24, [20/0], 1m6s, eBgp+
5000:0:0:6::/64, attached
    *via 2000:25::200, Ve 25, [20/0], 1m6s, eBgp+
5000:0:0:7::/64, attached
    *via 2000:26::200, Ve 26, [20/0], 1m6s, eBgp+
5000:0:0:8::/64, attached
    *via 2000:27::200, Ve 27, [20/0], 1m6s, eBgp+
5000:0:0:9::/64, attached
    *via 2000:28::200, Ve 28, [20/0], 1m6s, eBgp+
```

History

Release version	Command history
5.0.0	This command was introduced.

show ipv6 route system-summary

Displays IPv6 route information with respect to route limits and next-hop limits, as well as additional information, for all VRFs and specific VRFs.

Syntax

show ip route system-summary [**rbridge-id** *rbridge-id*] [**vrf** *name*]

Parameters

rbridge-id *rbridge-id*
Displays routes for a selected RBridge ID.

vrf *name*
Displays routes for a selected VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

show ip route summary vrf

Command Output

The **show ip route system-summary** command displays the following information:

Output field	Description
System Route Count	Displays current (all VRF aggregate) system-wide route count, the maximum value supported by the RBridge, and whether or not the system limit was exceeded in the past.
System Nexthop Count	Displays current (all VRF aggregate) system-wide next-hop count, the maximum value supported by the RBridge, and whether or not the system limit was exceeded in the past.
VRF-Name	Displays, on a per-VRF basis, the current route count on the VRF, the maximum number of routes (if configured) on the VRF, and a breakdown of routes as connected, static, per routing protocol, and so on. The display is for a named VRF, the default VRF, and the management VRF.

Examples

```
switch# show ipv6 route system-summary

System Route Count: 12192 Max routes: 20476 (Route limit not exceeded)
System Nexthop Count: 334 Max nexthops: 15360 (Nexthop limit not exceeded)

VRF-Name: 122_53
  Route count: 1033 Max routes: 2000 (Route limit not exceeded)
  18 connected, 1 static, 0 RIP, 1001 OSPF, 0 BGP, 0 ISIS

VRF-Name: abc
  Route count: 2006 Max routes: 2500 (Route limit not exceeded)
  2 connected, 0 static, 0 RIP, 2002 OSPF, 0 BGP, 0 ISIS

VRF-Name: default-vrf
  Route count: 3080 Max routes: Not Set (Route limit not exceeded)
  32 connected, 3 static, 0 RIP, 1011 OSPF, 2004 BGP, 0 ISIS

VRF-Name: mgmt-vrf
  Route count: 6 Max routes: Not Set (Route limit not exceeded)
  3 connected, 1 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS
```

History

Release version	Command history
5.0.1	This command was introduced.

show ipv6 static route

Displays information about IPv6 static routes.

Syntax

show ipv6 static route [*ipv6prefix* [**rbridge-id** { **all** | *rbridge-id* }] [**vrf** *vrf-name*] | **rbridge-id** { **all** | *rbridge-id* } | **vrf** *vrf-name*]

Parameters

ipv6prefix

IPv6 prefix in *A:B::/length* format.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

all

Specifies all RBridges in the cluster.

vrf *vrf-name*

Specifies a VRF instance.

all

Specifies all VRF instances.

default

Specifies the default VRF instance.

Modes

Privileged EXEC mode

Examples

The following example illustrates the output of the **show ipv6 static route** command:

```
switch# show ipv6 static route
IPv6 Configured Static Routes for VRF "default-vrf"
2014::/64-> 3001:1111::2000 preference: 1
   nh_vrf (default-vrf)
3ffe:1002::/64-> 2001::100 preference: 1
   nh_vrf (default-vrf)
   real-next-hop: 2001::100, interface: Te 7/0/48
2ffe:1111:2222::1234/128-> 3001::5678 preference: 1
   nh_vrf (default-vrf)
```

show ipv6 vrrp

Displays information about IPv6 VRRP and VRRP-E sessions.

Syntax

show ipv6 vrrp *VRID* [**detail**] [**summary**] [**rbridge-id** { *rbridge-id* | **all** }]

show ipv6 vrrp [**detail** | **summary**] [**rbridge-id** { *rbridge-id* | **all** }]

show ipv6 vrrp [**interface** { *<N>***gigabitethernet** [*rbridge-id*]*/slot/port* | **ve** *vlan_id* }] [**detail**] [**summary**]

show ipv6 vrrp rbridge-id { *rbridge-id* | **all** } [**detail**] [**summary**]

Parameters

VRID
The virtual group ID about which to display information. Valid values range from 1 to 128.

detail
Displays all session information in detail, including session statistics.

summary
Displays single line, session-information summaries.

rbridge-id { *rbridge-id* | **all** }
Displays information for a specified RBridge ID. If **all** is specified for the rbridge-id variable, information for all RBridge IDs is displayed.

interface
Displays information for an interface that you specify.

<N> **gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

ve *vlan_id*
Specifies the VE VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about IPv6 VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group, one or all RBridge IDs, or an interface for which to display VRRP output.

This command is for IPv6 VRRP and IPv6 VRRP-E. IPv6 VRRP-E supports only the VE interface type. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples

To show IPv6 VRRPv3 information in detail for a specific virtual group ID of 19, including session statistics:

```
switch# show ipv6 vrrp 19 detail
============Rbridge-id:122============
Total number of VRRP session(s)    : 1
VRID 19
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Backup
  Session Master IP Address: fe80::205:33ff:fe79:fb1e
  Virtual IP(s): 2001:2019:8192::1
  Virtual MAC Address: 02e0.5200.2513
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: ENABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Enabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                    Priority  Port Status
    =======                    ========  ===========
  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0
  Session Statistics:
  ===================
    Advertisements             : Rx: 103259, Tx: 1721
    Neighbor Advertisements              : Tx: 0
    Session becoming master    : 0
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
    VRRPE backup advt sent     : 1721
    VRRPE backup advt recvd    : 0
```

To show summary information for IPv6 VRRP-E statistics:

```
switch# show ipv6 vrrp summary
Total number of VRRP session(s)   : 2
Master session count  : 1
Backup session count  : 1
Init session count    : 0
VRID Session Interface  Admin   Current  State  Short-path Revert   SPF
                        State   Priority        Forwarding Priority Reverted
==== ======= =========  =====   ======== =====  ========== ======== ========
18   VRRPE   Ve 2018    Enabled 254      Master Enabled    unset    No
19   VRRPE   Ve 2019    Enabled 100      Backup Enabled    unset    No
```

show lacp

Displays Link Aggregation Control Protocol (LACP) statistics.

Syntax

show lacp [**counters** [*port-channel*] | **sys-id** [*port-channel*]

Parameters

counters

Displays LACP statistics for all port-channel interfaces.

port-channel

Displays counters for a specified port channel interface. Valid values range from 1 through 6144.

sys-id

Displays LACP statistics by system ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the LACP statistics for each port-channel interface for all port-channel interfaces or a single port-channel interface, or by system ID.

show lacp sys-id

Displays the Link Aggregation Control Protocol (LACP) system ID and priority information.

Syntax

show lacp sys-id

Modes

Privileged EXEC mode

Usage Guidelines

The system priority and the system Media Access Control (MAC) address make up the system identification. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC addresses associated with the system.

Examples

To display the local system ID:

```
switch# show lacp sys-id

% System 8000,00-05-1e-76-1a-a6
```

show license

Displays license information.

Syntax

show license [**rbridge-id** { *rbridge-id* | **all** }] [**all**]

Command Default

Displays the licenses installed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

all

Executes the command on all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the license information for the local switch or any switch in a Brocade VCS Fabric cluster. The command output includes the RBridge ID, license description, expiration if applicable, the feature name, and an indication of whether the license is valid. A string of "x" characters is displayed for the license key.

In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.

Examples

To display a Brocade VDX 8770 licensed for Advanced Services: (This configuration enables the use of Layer 3 and FCoE features. The VCS Fabric license is enabled on all VDX platforms by default starting with Network OS 4.1.0; a VCS Fabric license does not need to be installed to enable VCS Fabric functionality.)

```
switch# show license

rbridge-id: 60
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       Advanced Services license
       Feature name:ADVANCED_SERVICES
       License is valid
```

Related Commands

license add, license remove, show license id

show license id

Displays the RBridge License ID.

Syntax

show license id [**rbridge-id** { **rbridge-id** { *rbridge-id* | **all** }] [**all**]

Command Default

Displays the license ID installed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

all

Executes the command on all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the RBridge license ID (WWN) for the specified switch. You need the RBridge license ID when you prepare to add a license.

In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.

Examples

To display the license ID for the local switch:

```
switch# show license id

Rbridge-Id       LicenseId
========================================
2                10:00:00:05:1E:00:4C:80
```

Related Commands

license add, license remove, show license

show linecard

Displays information about the line cards present in the chassis.

Syntax

show linecard

Modes

Privileged EXEC mode

Command Output

The **show linecard** command displays the following information:

Output field	Description
Slot	Displays the slot number. Slots for line cards are L1 through L4 on Brocade VDX 8770-4 switches, and L1 through L8 on Brocade VDX 8770-8 switches.
Type	Displays the line card type.
Description	Module description.
ID	Displays IDs for line cards.
Status	Displays the status of the line card as one of the following: • VACANT - The slot is empty. • POWERED-OFF - The module is present in the slot but is powered off. • POWERING UP - The module is present and powering on. • LOADING - The module is present, powered on, and loading the initial configuration. • DIAG RUNNING POST1 - The module is present, powered on, and running the POST (power-on self-test). • DIAG RUNNING POST2 - The module is present, powered on, and running the reboot power on self tests. • INITIALIZING - The module is present, powered on, and initializing hardware components. • ENABLED - The module is on and fully enabled. • DISABLED - The module is powered on but disabled. • FAULTY - The module is faulty because an error was detected. • UNKNOWN - The module is inserted but its state cannot be determined.

Examples

To display the line cards present in a Brocade VDX 8770-4 switch:

```
switch# show linecard

Slot  Type         Description                ID      Status
--------------------------------------------------------------------
 L1   LC48X10G     48-port 10GE card          114     ENABLED
 L2   LC48X10G     48-port 10GE card          114     ENABLED
 L3                                           VACANT
 L4   LC48X1G      48-port 1GE card           131     ENABLED
```

Related Commands

linecard, show sfm, show slots

show lldp interface

Displays the LLDP status on the specified interface.

Syntax

show lldp interface [<*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display all the LLDP interface information for a selected interface:

```
switch# show lldp interface tengigabitethernet 1/0/0

LLDP information for Te 1/0/0
  State:                    Enabled
  Mode:                     Receive/Transmit
  Advertise Transmitted:    30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:           1 seconds
  DCBX Version :            CEE
  Auto-Sense :              Yes
  Transmit TLVs:            Chassis ID               Port ID
                            TTL                      System Name
                            IEEE DCBx                DCBx FCoE App
                            DCBx FCoE Logical Link
  DCBx FCoE Priority Values: 3
  DCBx iSCSI Priority Values: 4
```

To display all the LLDP interface information:

```
switch# show lldp
LLDP Global Information
  system-name: switch
  system-description: Brocade-VDX-VCS 100
  description:
  State:                    Enabled
  Mode:                     Receive/Transmit
  Advertise transmitted:    30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:           1 seconds
  Transmit TLVs:            Chassis ID               Port ID
                            TTL                      System Name
                            IEEE DCBx                DCBx FCoE App
                            DCBx FCoE Logical Link
  DCBx FCoE Priority Values: 3
  DCBx iSCSI Priority Values: 4
```

show lldp neighbors

Displays LLDP information for all neighboring devices on the specified interface.

Syntax

show lldp neighbors [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* } **detail**]

Parameters

interface

Specifies an Ethernet interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

detail

Displays all the LLDP neighbor information in detail for the specified interface.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display LLDP information for all neighboring devices on the specified interface.

ATTENTION

If you do not use the **interface** parameter, only the mandatory TLVs are displayed.

Examples

To display detailed LLDP neighbor information on a specific interface:

```
switch# show lldp neighbors interface tengigabitethernet 3/0/8 detail

Neighbors for Interface Te 3/0/8
MANDATORY TLVs
===============
Local Interface: Te 0/8    Remote Interface: Te 3/0/8 (IF Name)
Dead Interval: 120 secs  Remaining Life : 100 secs Tx: 536  Rx: 535
Chassis ID: 0005.1e76.1020 (MAC)
Remote Mac: 0005.1e76.102c
OPTIONAL TLVs
==============
Port Interface Description: Te 3/0/8
System Name: sw0
System Description: Fibre Channel Switch.
System Capabilities: Switching Routing
System Capabilities Enabled: Switching
Link Prim: 257
Remote Protocols Advertised:  Multiple Spanning Tree Protocol
Remote VLANs Configured: VLAN ID: 1  VLAN Name: default
AutoNego Support: Supported Not Enabled
AutoNego Capability: 0
Operational MAU Type: 0
Link Aggregation Capability: Capable
Link Aggregation Status: Disabled
Port Vlan Id: 1
Port & Protocol Vlan Flag: Supported Not enabled
Port & Protocol Vlan Id: 0
Link Aggregation Port Id: 0
Max Frame Size: 2500
Management Address: 10.32.152.21 (IPv4)
Interface Numbering: 2
Interface Number: 0x4080100 (67633408)
OID: 0x100f99b4
```

show lldp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

Syntax

show lldp statistics [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* }]

Parameters

interface

Specifies an Ethernet interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify an interface, this command displays the LLDP statistics for all interfaces.

Examples

To display LLDP statistics on the specified interface:

```
switch# show lldp statistics interface tengigabitethernet 5/0/8

LLDP Interface statistics for Te 5/0/8
Frames transmitted: 555
Frames Aged out:    0
Frames Discarded:   0
Frames with Error:  0
Frames Recieved:    554
TLVs discarded:     0
TLVs unrecognized:  0
```

show logging auditlog

Displays the internal audit log buffer of the switch.

Syntax

show logging auditlog [**count** *count*] [**reverse**] [**rbridge-id** *rbridge-id* | **all**]

Parameters

count *count*

Specifies the number of messages to display.

reverse

Displays the audit log in reverse order.

rbridge-id *rbridge-id*

Specifies an RBridge.

all

Executes the command on all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To display the audit log messages stored in the internal buffer:

```
switch# show logging auditlog

0 AUDIT,2012/04/13-02:35:59 (GMT), [DCM-2002], INFO, DCMCFG, admin/admin/10.72.16.41/ssh/cli,, chassis,
Event: noscli exit, Status: success, Info: Successful logout by user [admin].
1 AUDIT,2012/04/13-02:43:23 (GMT), [DCM-2001], INFO, DCMCFG, admin/admin/10.72.16.41/ssh/cli,, chassis,
Event: noscli start, Status: success, Info: Successful login attempt through ssh from 10.72.16.41.
```

Related Commands

clear logging auditlog, clear logging raslog, log-dampening-debug

show logging raslog

Displays the internal RASlog buffer of the switch.

Syntax

show logging raslog [**attribute** *attribute*] [**blade** *blade*] [**count** *count*] [**message-type** *type*] [**reverse**] [**severity** *severity*] [**rbridge-id** *rbridge-id*]

Parameters

attribute *attribute*
Filters output by message attribute. Valid attributes include FFDC and VCS.

blade *blade*
Displays for the specified blade only. Valid values for blade include MM1, MM2, and LC[1-8].

count *count*
Specifies the number of messages to display.

message-type *type*
Filters the output by message type. Valid message types include DCE or SYSTEM.

severity *severity*
Filters the output by message severity. Valid severity levels include the following: critical, error, info, and warning.

reverse
Displays the messages in reverse order.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use the filters to customize the output.

This command is supported only on the local switch.

The RASLog messages contain the module name, error code, and message details.

Examples

To display all RASLog messages stored in the system:

```
switch# show logging raslog

NOS: 3.0.0
2012/05/25-17:37:15, [LOG-1003], 1, M1, INFO, VDX8770-4, SYSTEM error log has been cleared
2012/05/25-17:38:32, [SEC-1203], 3, M1, INFO, sw0, Login information: Login successful via TELNET/SSH/
RSH. IP Addr: 10.24.65.24
2012/05/25-17:42:54, [SEC-1203], 4, M1, INFO, sw0, Login information: Login successful via TELNET/SSH/
RSH. IP Addr: 10.24.65.24
2012/05/25-17:43:12, [IPAD-1002], 5, M1, INFO, VDX8770-4, Switch name has been successfully changed to
dutA1-sw0.
2012/05/25-17:51:42, [FW-1439], 180, M1, WARNING, dutA1-sw0, Switch status change contributing factor
Switch offline.
(Output truncated)
```

To display all RASLog messages for a line card:

```
switch# show logging raslog blade LC2

NOS: 3.0.0
2012/05/28-12:07:41, [HASM-1004], 822, L2, INFO, VDX8770-4, Processor rebooted - Reset
2012/05/28-12:07:41, [HASM-1104], 823, L2, INFO, VDX8770-4, Heartbeat to M1 up
2012/05/28-12:07:48, [HASM-1108], 830, L2, INFO, VDX8770-4, All service instances become active.
2012/05/29-13:32:50, [HASM-1004], 2721, L2, INFO, VDX8770-4, Processor rebooted - Reset
```

To display warning messages only on the standby management module:

```
switch# show logging raslog blade MM1 severity warning

NOS: 3.0.0
2012/03/09-15:20:55, [FW-1042], 26, M1, WARNING, dutA1-sw0, Sfp TX power for port 1/2/9, is below low
boundary(High=1999, Low=125). Current value is 17 uW.
2012/03/09-15:20:55, [FW-1046], 27, M1, WARNING, dutA1-sw0, Sfp Current for port 1/2/9, is below low
boundary(High=10, Low=3). Current value is 0 mA.
2012/03/09-15:20:55, [FW-1042], 28, M1, WARNING, dutA1-sw0, Sfp TX power for port 1/2/17, is below low
boundary(High=1999, Low=125). Current value is 18 uW.
(Output truncated)
```

To display only the FFDC messages:

```
switch# show logging raslog attribute FFDC rbridge-id 1

NOS: 3.0.0
1970/01/01-00:09:43, [HASM-1200], 106, MM1 | FFDC, WARNING, chassis, Detected termination of process
Dcmd.Linux.powe:1660
```

Related Commands

clear logging raslog, logging raslog console

show mac-address-table

Displays forwarding information for all MAC addresses, for a specific dynamic or static MAC address, for all dynamic MAC addresses, for all static MAC addresses, for a specific interface, for a specific VLAN, or for MAC addresses associated with port profiles.

Syntax

show mac-address-table [**address** *mac-addr* | **aging-time** [**conversational** [**rbridge-id**] *rbridge-id*]] | **count** [**address***MAC_address* | **conversational linecard** *linecard_number* [**address** [*MAC_address* | **rbridge-id** *rbridge-id*]] | **interface** {*<N>* **gigabitethernet** *rbridge-id/slot/port* | **vlan***vlan_id* } | **dynamic** [**address** *MAC_address* | **interface** {*<N>* **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **tunnel** *number* | **vlan** *vlan_id*] | **interface** { *<N>* **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **tunnel** *number* | **vlan** *vlan_id* } | **static** [**address** *MAC_address* | **interface** {*<N>* **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **tunnel** *number* | **vlan** *vlan_id*] | **vlan** *vlan_id* | **dynamic** | **interface** | **learning-mode** [**rbridge-id** [*rbridge-id*]] | **linecard interface** |**port-profile** [**address***MAC_address* | **count** | **dynamic** | **vlan***vlan_id*] | **static** | **vlan***vlan_id*]

Parameters

address *MAC_adddress*
Displays forwarding information for a 48-bit MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

aging-time
Displays the aging time.

conversational
Displays conversational MAC learning (CML) aging time, or is used for forwarding entries.

rbridge-id [*rbridge-id*]
Specifies the RBridge ID display.

count
Displays the count of forwarding entries.

address *MAC_address*
Specifies a MAC address.

conversational linecard *linecard_number*
Specifies CML addresses for a line card.

address
Specifies a MAC address or an RBridge.

interface
Specifies a physical interface or VLAN.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id[*rbridge-id*]
Specifies all RBridge IDs or a single RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel number. Range is from 1 through 6144.

tunnel *number*
Specifies a tunnel. Range is from 1 through 100000.

dynamic
Specifies dynamic (legacy) MAC addresses for a physical interface, port-channel, or VLAN.

static
Specifies static MAC addresses for a physical interface, port-channel, or VLAN.

learning-mode
Specifies the learning mode for all RBridges or one RBridge.

linecard interface
Specifies a line card.

port-profile
Specifies a port profile.

Modes

Privileged EXEC mode

Examples

To display a specific MAC address in the table:

```
switch# show mac-address-table address 0011.2222.3333

vlanId   Mac-address       Type     State      Ports
100      0011.2222.3333    Static   Inactive   Te 0/1
Total MAC addresses   : 1
```

To display the aging time for a specific MAC address table:

```
switch# show mac-address-table aging-time

MAC Aging-time : 300 seconds
```

To display a dynamic MAC address table:

```
switch# show mac-address-table dynamic

vlanId   Mac-address       Type     State      Ports
100      0011.2222.5555             Dynamic     Inactive      Te 0/1
100      0011.2222.6666       Dynamic  Inactive   Te 0/1
Total MAC addresses   : 2
```

show media

Displays the SFP information for all the interfaces present on a switch.

Syntax

show media

Modes

Privileged EXEC mode

Usage Guidelines

The command output will be several pages long.

The TX Power Field in the **show media** command is not supported by the 40-Gbps optics.

Examples

To display all SFP information:

```
switch# show media
Interface Ten Gigabit Ethernet 0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 10_GB/s
  Name           id
  Encoding       6
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     8   (units 10 meters)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     42:52:4f
  Vendor PN      57-0000075-01
  Vendor Rev     A
  Wavelength     850 (units nm)
  Options        001a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max         0
  BR Min         0
  Serial No      AAA108454100431
  Date Code      081108
  Optical Monitor yes
  Temperature    44 Centigrade
  Voltage        3246.8  (Volts)
  Current        0.002  (mAmps)
  TX Power       0.1  (uWatts)
  RX Power       0.1  (uWatts)
(Output truncated)
```

Related Commands

show media interface, show media linecard

show media interface

Displays the SFP information for a specific interface.

Syntax

show media interface [<*N*>**gigabitethernet** *rbridge-id/slot/port* | **fibrechannel** *rbridge-id/slot/port*]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

fibrechannel *rbridge-id/slot/port*

Specifies a valid external 1-gigabit FibreChannel interface.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The **fibrechannel** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6740 switches.

Examples

To display SPF information for a 1-gigabit Ethernet interface:

```
switch# show media interface gigabitethernet 1/0/1

  Interface       Gigabit Ethernet 0/1
  Identifier      2    On-board
  Connector       34   CAT-5 copper cable
  Transceiver     1000 BASE-T Gigabit Ethernet
  Name            cu
  Encoding        5    IEEE 802.3ab
  Length          max 100 m
  Copper Speed    1GB/s Fixed
  Copper Duplex   Full Duplex
  Sync status     Valid/No
  Vendor Name     Broadcom
  Vendor OUI      00:1B:E9
  Vendor model    02:0F
  Vendor Rev      01
  Options         001a Remote fault/Jabber detect/copper link up
  Temperature threshold/val    55 Centigrade
  Voltage threshold/val        3289.9  (mVolts)
```

To display SFP information for a 10-gigabit Ethernet interface:

```
switch# show media interface tengigabitethernet 5/0/1

Interface Ten Gigabit Ethernet 5/0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 10_GB/s
  Name           id
  Encoding       6
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     8   (units 10 meters)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1E
  Vendor PN      57-0000075-01
  Vendor Rev     A
  Wavelength     850 (units nm)
  Options        001a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max         0
  BR Min         0
  Serial No      AAA108454100431
  Date Code      081108
  Temperature    44 Centigrade
  Voltage        3246.8  (Volts)
  Current        0.002  (mAmps)
  TX Power       0.1  (uWatts)
  RX Power       0.1  (uWatts)
```

To display SFP information for a Fibre Channel interface:

```
switch# show media interface fibrechannel 66/0/1

  Interface         FibreChannel 66/0/1
  Identifier        3    SFP
  Connector         7    LC
  Transceiver       540c404040000000 200,400,800_MB/s M5,M6 sw Short_dist
  Encoding          1    8B10B
  Baud Rate         85   (units 100 megabaud)
  Length 9u         0    (units km)
  Length 9u         0    (units 100 meters)
  Length 50u        5    (units 10 meters)
  Length 62.5u      2    (units 10 meters)
  Length Cu         0    (units 1 meter)
  Vendor Name       BROCADE
  Vendor OUI        00:05:1e
  Vendor PN         57-1000012-01
  Vendor Rev        A
  Wavelength        850  (units nm)
  Options           003a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max            0
  BR Min            0
  Serial No         UAF110170000VP1
  Date Code         100422
  DD Type           0x68
  Enh Options       0xfa
  Status/Ctrl       0x82
  Alarm flags[0,1]  0x5, 0x40
  Warn Flags[0,1]   0x5, 0x40
                                          Alarm                Warn
                                     low          high     low          high
Temperature   28      Centigrade     -10          90       -5           85
Voltage       3331.4  mVolts        2900.0       3700.0   3000.0       3600.0
Current       0.310   mAmps            1.000       17.000      2.000       14.000
TX Power      -21.7   dBm (6.8 uW)    125.9 uW    631.0 uW   158.5 uW    562.3 uW
RX Power      -inf    dBm (0.0 uW)     10.0 uW   1258.9 uW    15.8 uW   1000.0 uW
```

Related Commands

show media, show media linecard

show media linecard

Displays the SFP information for a specified line card.

Syntax

show media linecard *number*

Parameters

number

Numeric identifier for the line card.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a summary of small form-factor pluggable (SFP) and Quad SFP media information for each interface on the specified module.

This command is supported only on the local RBridge.

Examples

To display the SFP media information for an LC48X10G line card in slot 2:

```
switch# show media linecard 2

Interface      Ten Gigabit Ethernet 1/2/1
  Identifier     3    SFP
  Connector      33   Copper Pigtail
  Transceiver            d580884104000002 10_GB/s TW Short_dist
  Name           cu
  Encoding       0
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     0   (units 10 meters)
  Length 62.5u   0   (units 10 meters)
  Length Cu      1   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1e
  Vendor PN      58-1000026-01
  Vendor Rev     A
  Wavelength     3072(units nm)
  Options        0012
  BR Max         0
  BR Min         0
  Serial No      CAMB110100607EW
  Date Code      110111
  Optical Monitor No
  Temperature    N/A
  Voltage        N/A
  Current        N/A
  TX Power       N/A
  RX Power       N/A
(Output truncated)
```

To display the Quad SFP media information for an LC12X40G line card in slot 3:

```
switch# show media linecard 3

Interface      fortygigabitethernet 1/3/2
  Identifier     13   QSFP
  Connector      12
  Transceiver            0000000000000004 40_GB/s  Short_dist
  Name           sw
  Encoding       5    IEEE 802.3ab
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      50  (units 100 meters)
  Length 50u     0   (units 10 meters)
  Length 62.5u   0   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    5ROCADE
  Vendor OUI     00:05:1e
  Vendor PN      57-1000128-01
  Vendor Rev     A
  Wavelength     17000(units nm)
  Options        0000
  BR Max         15
  BR Min         222
  Serial No      LTA111421000923
  Date Code      111022
  Optical Monitor yes
  Temperature    31 Centigrade
  Voltage        3313.2  (mVolts)
  Current        7.204  (mAmps)
  TX Power       N/A
  RX Power       0.0  (uWatts)
```

Related Commands

linecard, show slots

show mm

Displays information about the Management Modules present in the chassis.

Syntax

show mm

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic tests (POST1, POST2) are not running on the management modules.

Command Output

The **show mm** command displays the following information:

Output field	Description
Slot	Displays the slot number. Slots for management modules are M1 and M2.
Type	Displays the line card type. The management module type is MM.
Description	Module description
ID	Displays the module ID. The ID for the management module is 112.
Status	Displays the status of the module as one of the following: • VACANT - The slot is empty. • POWERED-OFF The module is present in the slot but is powered off. • POWERING UP - The module is present and powering on. • LOADING - The module is present, powered on, and loading the initial configuration. • INITIALIZING - The module is present, powered on, and initializing hardware components. • ENABLED - The module is on and fully enabled. • DISABLED - The module is powered on but disabled. • FAULTY - The module is faulty because an error was detected. • UNKNOWN - The module is inserted but its state cannot be determined.

Examples

To display the management modules present in a Brocade VDX 8770-4 chassis:

```
switch# show mm

Slot  Type         Description                ID      Status
-------------------------------------------------------------------
 M1   MM           Management Module          112     ENABLED
 M2                                                    VACANT
```

Related Commands

show linecard, show sfm, show slots

show monitor

Displays the monitoring information for all Port Mirroring sessions or for a single session.

Syntax

show monitor [**session** *session_number*]

Parameters

session *session_number*

Specifies a session identification number. Valid values range from 0 through 511.

Modes

Privileged EXEC mode

Examples

To display monitoring information for all Port Mirroring sessions:

```
switch# show monitor

Session                         :1
Type                      :Remote source session
Description                     :Test monitor session
State                           :Enabled
Source interface                :Te 1/0/10 (Up)
Destination interface           :Vlan x
Direction                       :Rx
```

Related Commands

monitor session

show name-server brief

Displays brief entries of local name server (NS) information about devices connected to a switch.

Syntax

show name-server brief [**rbridge-id** *rbridge-id*]

Command Default

If no RBridge ID is specified, brief entries for all devices in the fabric are displayed.

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Brief output lists only the Fibre Channel address (PID) of each device.

NOTE
If no information is available for the switch, the command displays the message: "0 entries."

Examples

```
switch# show name-server brief
```

Example output, wtih no hidden entries, follows; note that there are two spaces preceding each PID:

```
481000  481040  471000  471040
4 entries
```

Hidden entries are preceded by a single space, followed by an asterisk [*]. Output from RBridge 0x47 perspective (PID 471080 hidden, PID 481000 removed) follows:

```
471040 *471080  481040
2 entries
* 1 hidden entries due to duplicate WWN
```

Related Commands

show name-server detail, show name-server nodefind

show name-server detail

Displays local name server (NS) information about devices connected to a switch.

Syntax

show name-server detail [**rbridge-id** *rbridge-id*]

Command Default

If no RBridge ID is specified, detailed entries for all devices in the fabric are displayed.

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Command Output

The **show name-server detail** command displays the following information:

Output field	Description
PID	Fibre Channel address of the device in 6-digit hexadecimal format.
Port Name	Worldwide port name (WWPN) of the device.
Node Name	Worldwide node name (WWNN) of the device.
SCR	Indicates the State Change Registration of the device, which affects RSCN behavior. The value can be one of the following: • 0: No registration • 1: Fabric detected RSCN • 2: Port detected RSCN • 3: Both Fabric and Port detected RSCN NOTE This information is only available for devices that are connected to the local RBridge on which the command is executed.
FC4s	Fibre Channel FC4 type of the device represented as an ASCII string.
PortSymb	User defined name for this port (ASCII string).
Fabric Port Name	Fabric port name (worldwide name format). This is the F_Port worldwide name to which the N_Port connects.
Permanent Port Name	Physical Nx_Port worldwide name.
Device Type	Type and role of the device, where the device type is either "Physical", "Virtual", "NPIV", or "iSCSI". The role is either "Initiator", "Target", or "Initiator + Target". If the device role is not

Output field	Description
	registered, the display indicates "unknown". If the device registers a type that is not one of the aforementioned values, then the type is listed as "undefined".
Interface	Interface information for the port. For FCoE devices this information is shown as: Fcoe vlan/ rbridge-id/FCoE port.
Physical Interface	Physical interface information for the port. For FCoE devices this information is shown as: Te rbridge-id/slot/port Where Te = Ten gigabit Ethernet.
Share Area	The state of the Brocade shared area addressing method. If "Yes" then the port uses shared area addressing.
Redirect	Indicates whether or not the device is involved in Brocade Frame Redirection. If "Yes" then the device is involved in Frame Redirection zoning.

If no information is available for the switch, the command displays the message: "total number of 0 entries."

For each detail entry displayed, if the device has been flagged as having a duplicate Port WWN, the following text appears after the entry:

```
*** Duplicate Port WWN entry - PID: <PID>
 *** Please see RAS log entry NS-1012 pertaining to this device
```

Examples

To view name server entries for all devices connected to a switch:

```
switch# show name-server detail

PID: 012100
Port Name: 10:00:00:05:1E:ED:95:38
Node Name: 20:00:00:05:1E:ED:95:38
SCR: 3
FC4s: FCP
PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat
Enterprise Linux Server release 5.5"
NodeSymb: NULL
Fabric Port Name: 20:21:00:05:1E:CD:79:7A
Permanent Port Name: 10:00:00:05:1E:ED:95:38
Device type: Physical Initiator
Interface: Fcoe 1/1/9
Physical Interface: Te 1/0/9
Share Area: No
Redirect: No
```

Related Commands

show name-server brief, show name-server nodefind

show name-server nodefind

Displays the local name server (NS) information for a specific device.

Syntax

show name-server nodefind { **PID** *pid* | **WWN** *wwn* }

Parameters

PID *pid*

Specifies the Fibre Channel address of the device to search for.

WWN *wwn*

Specifies the World Wide Name (WWN) of the device to search for.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display local name server (NS) information about a specific detailed entry.

The lookup is performed using either the Fibre Channel address (Port ID, or PID), or the WWN of the device. If no information is available for the device, the command displays one of the following messages:

- For PID lookup: `Device with PID of pid does not exist`
- For WWN lookup: `Device with WWN of wwn does not exist`

Refer to **show name-server detail** for descriptions of the displayed information.

Examples

To view name server information for a device specified by PID:

```
switch# show name-server nodefind pid 0x012100

PID: 012100
Port Name: 10:00:00:05:1E:ED:95:38
Node Name: 20:00:00:05:1E:ED:95:38
SCR: 3
FC4s: FCP
PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat
Enterprise Linux Server release 5.5"
NodeSymb: NULL
Fabric Port Name: 20:21:00:05:1E:CD:79:7A
Permanent Port Name: 10:00:00:05:1E:ED:95:38
Device type: Physical Initiator
Interface: Fcoe 1/1/9
Physical Interface: Te 1/0/9
Share Area: No
Redirect: No
```

Related Commands

show name-server brief, show name-server detail

show name-server zonemember

Displays the local name server (NS) zoning information.

Syntax

show name-server zonemember { **PID** *pid* | **WWN** *wwn* }

Parameters

PID *pid*

Specifies the Fibre Channel address of the device.

WWN *wwn*

Specifies the World Wide Name (WWN) of the device.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display detailed local name server (NS) information about all devices zoned with the specified device. The lookup is performed using either the Fibre Channel address (Port ID, or PID), or the WWN of the device.

If no information is available for the device, the command displays one of the following messages:

- For PID lookup: `Device with PID of pid does not exist`
- For WWN lookup: `Device with WWN of wwn does not exist`

If the specified device has been flagged as having a duplicate Port WWN, the following text is displayed:

```
Device with duplicate WWN removed from Name Server database: <device detail entry displayed here>
Please review RAS log for NS-1012 entries in order to obtain details about the conflicting device pair.
```

Examples

To view name server information for a device specified by PID:

```
switch# show name-server zonemember pid 0x010500

PID: 010500
Port Name: 10:00:00:05:1F:ED:95:38
Node Name: 20:00:00:05:1F:ED:95:38
SCR: 3
FC4s: FCP
PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat
Enterprise Linux Server release 5.5"
NodeSymb: NULL
Fabric Port Name: 20:21:00:05:1F:ED:79:7A
Permanent Port Name: 10:00:00:05:1F:ED:95:38
Device type: Physical Initiator
Interface: Fcoe 1/1/5
Physical Interface: Te 1/0/5
Share Area: No
Redirect: No
PID: 010600
Port Name: 10:00:00:05:1F:CD:95:38
Node Name: 20:00:00:05:1F:CD:95:38
SCR: 3
FC4s: FCP
PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat
Enterprise Linux Server release 5.5"
NodeSymb: NULL
Fabric Port Name: 20:21:00:05:1E:CD:79:7A
Permanent Port Name: 10:00:00:05:1E:CD:95:38
Device type: Physical Initiator
Interface: Fcoe 1/1/6
Physical Interface: Te 1/0/6
Share Area: No
Redirect: No
```

Related Commands

show name-server brief, show name-server detail, show name-server nodefind

show nas statistics

Displays automatic network attached storage (Auto NAS) statistics.

Syntax

show nas statistics all | **server-ip** *ip_addr/prefix* [**vlan** *VLAN_id* | **vrf** *VRF_name*] [**rbridge-id** *rbridge-id*]

Parameters

all

Shows all gathered statistics.

server-ip

IP address to show Auto NAS statistics for.

ip_addr/prefix

IPv4 address/prefix of a specified **Auto** NAS port.

vlan *VLAN_id*

Specifies which VLAN interface to display the statistics for.

vrf *VRF_name*

Specifies which VRF interface to display the statistics for.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Related Commands

backup-advertisement-interval, clear nas statistics, nas auto-qos, nas server-ip, show running-config nas server-ip, show system internal nas, show cee maps

show netconf client-capabilities

Displays the client capabilities associated with each NETCONF session.

Syntax

show netconf client-capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display client capabilities for all active NETCONF sessions. It always displays the session-ID, login name of the user of the client session, the host IP address, and the time the user logged on. The application vendor name, application product name and version number, and the identity of the client are also returned if these values are advertized by the client as capabilities in the <hello> message to the server at the start of the session.

Examples

```
switch# show netconf client-capabilities

Session Id  : 10
User name   : root
Vendor      : Brocade
Product     : Brocade Network Advisor
Version     : 9.1.0 Build 123
Client user : admin-user
Host IP     : 10.24.65.8
Login time  : 2011-08-18T08:54:24Z
Session Id  : 11
User name   : root
Vendor      : Not Available
Product     : Not Available
Version     : Not Available
Client user : Not Available
Host IP     : 10.24.65.8
```

Related Commands

show netconf-state capabilities, show netconf-state statistics

show netconf-state capabilities

Displays NETCONF server capabilities.

Syntax

show netconf-state capabilities

Modes

Privileged EXEC mode

Examples

```
switch# show netconf-state capabilities

netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:writable-running:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability http://tail-f.com/ns/netconf/actions/1.0
netconf-state capabilities capability http://tail-f.com/ns/aaa/1.1?revision=2010-06-17&module=tailf-aaa
netconf-state capabilities capability urn:brocade.com:mgmt:brocade-aaa?
revision=2010-10-21&module=brocade-aaa
(Output truncated)
```

Related Commands

show netconf client-capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state sessions, show netconf-state statistics

show netconf-state datastores

Displays the NETCONF datastores that are present on the NETCONF server along with related locking information.

Syntax

show netconf-state datastores

Modes

Privileged EXEC mode

Examples

```
switch# show netconf-state datastores

         LOCKED                  LOCKED
         BY       LOCKED  LOCK   BY       LOCKED          LOCKED
NAME     SESSION  TIME    ID     SESSION  TIME    SELECT  NODE
-------------------------------------------------------------------
running  -        -
startup  -        -
```

Related Commands

show netconf-state capabilities, show netconf-state schemas, show netconf-state sessions, show netconf-state statistics

show netconf-state schemas

Displays the data models supported by the NETCONF server.

Syntax

show netconf-state schemas

Modes

Privileged EXEC mode

Related Commands

show netconf-state capabilities, show netconf-state datastores, show netconf-state sessions, show netconf-state statistics

show netconf-state sessions

Displays information about currently active NETCONF sessions.

Syntax

show netconf-state sessions

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the following information about each active NETCONF session:

- Transport used by the session
- Login name of the user
- Client IP address
- The time the user logged in

This command also provides a summary of RPC error counts and notifications.

Examples

```
switch# show netconf-state sessions

etconf-state sessions session 6
transport cli-console
username admin
source-host 127.0.0.1
login-time 2011-09-05T11:29:31Z
netconf-state sessions session 9
transport netconf-ssh
username root
source-host 172.21.132.67
login-time 2011-09-05T11:50:33Z
in-rpcs 0
in-bad-rpcs 0
out-rpc-errors 0
out-notifications 0
```

Related Commands

show netconf-state capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state statistics

show netconf-state statistics

Displays NETCONF server statistics.

Syntax

show netconf-state statistics

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display statistics related to the NETCONF server, including counts of the following entities:

- Start time of the NETCONF server
- Erroneous <hello> elements received
- Client sessions begun
- Dropped sessions
- Remote procedure calls (RPCs) received
- Erroneous RPCs received
- RPC errors returned to clients
- Notifications sent

Examples

```
switch# show netconf-state statistics

netconf-state statistics netconf-start-time 2012-04-27T09:12:09Z
netconf-state statistics in-bad-hellos 0
netconf-state statistics in-sessions 3
netconf-state statistics dropped-sessions 0
netconf-state statistics in-rpcs 4
netconf-state statistics in-bad-rpcs 0
netconf-state statistics out-rpc-errors 0
netconf-state statistics out-notifications 0
```

Related Commands

show netconf-state capabilities, show netconf-state datastores, show netconf-state schemas, show netconf-state sessions

show notification stream

Displays notifications about the event stream.

Syntax

show notification stream

Modes

Privileged EXEC mode

show nsx controller

Displays connection status and statistics for the NSX controller.

Syntax

show nsx-controller [**brief** | **client-cert** | **name** *name*]

Parameters

brief

Shows a brief listing of NSX controller connections.

client-cert

Displays the public certificate used for the NSX controller connection.

name *name*

Displays the name of the NSX controller profile that has been configured.

Modes

Privileged EXEC mode

Usage Guidelines

This command is available only for a switch that is in logical chassis cluster mode.

Command Output

The **show nsx controller** command displays the following information:

State	Meaning
Connected	Connection is up and operational.
Not activated	User has shut down the connection.
Connection in progress	Switch is attempting to connect to the NSX controller.
Connection lost	Disconnected by peer, or network reachability has been lost. The switch will automatically attempt to connect after the configured amount of reconnect-interval seconds.
Connection dead	Switch could not connect to the NSX controller after the maximum number of reconnect attempts. The user can restart the connection via the "nsx-controller reconnect" command (Privileged EXEC mode) or via the "no activate" and "activate" commands in NSX Controller configuration mode.

Examples

To show the status of the NSX controller:

```
sw0# show nsx-controller
NSX controller cluster "yy"
Seed IP address 192.168.0.13, port 6632, method SSL
Reconnect interval 10 secs, Max retries 100
Admin state up, Number of connections 1
Number of tunnels 2, Number of MACs 4
Connection details:
    ID fb580822-b185-4068-8c9b-f15a800b4eea, Connected
    IP address 192.168.0.13, port 6632, method SSL
    Reconnect interval 10000 millis, Number of retries 0 (max 100)
    Last connect time: Wed Jan 29 16:33:48 2014
    Last disconnect time: Wed Jan 29 16:33:48 2014
```

To show a brief listing of NSX controller connections:

```
sw0# show nsx-controller brief
Controller name      IP address      Port Type Connection state
==================== =============== ==== ==== ======================
yy                   192.168.0.13    6632 SSL  Connected
```

To display the public certificate used for the NSX controller connection:

```
sw0# show nsx-controller client-cert
-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoTB0Jyb2NhZGUxEjAQBgNVBAMTCWxvY2FsaG9zdDAeFw0xNDAxMjkxNjMyMDZa
Fw0xNTAxMjkxNjMyMDZaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKEwdCcm9jYWRl
MRIwEAYDVQQDEwlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCtVSTo/ZYpA591cuSGoNRiT7mPHUzn5SUyTTM6J4ZlFErYtD5iLmjZbiU4
hUd45tnSYPgSxts4oARklAobAdj1KS/Y4WuVXgQWSqQf4mLEnO5ONsaZHGt+I/TV
SL4DWqfZ/SMOYpDPW326iN6I9JI0MctcDPNm49pmroAZkePxC1zuAh5LAkYIGsga
1/5gGWX2GkT0Jv5inljZ43rsNpVUzylb+wTrhUbWlAFx6y6wZtAdNWz8mpoguV8E
WB7W4woltqyAu0X8OkGOcwnyRmrG/eu4PmTkBxpOQnsHfkEtLlnbu3Nt9l6v8gKn
/0mi+tS22+2jdH9OzWMuSVOvxt5pAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBABj2
rjDhCiByiwl65SODhlFy5+z8Pi/m4aCAlNH1yI9EteRC7nbYs94wu6DuJ5LaET3l
JWtKjY0aZ2Um0Sg9ll3aG9+kkaVtn3oMgAre7/pRxuxssId7PuLibYqfzlzuwtwa
wVbtsrxUwZYW55mFOI7+ACMQKq3WUUb8Sl4vrNq+gB49kPJAQSYaygHZ+FdPYd01
j7B2L495jaXBtkttz/hai5BGqKwnfxlSqH0pI+RLrEvJrUHbwIMUNAcBODRZqxnX
0WmnxW5IIynvyRZAx6AH3EdCWjkMXA3/D8VQ/eDoYNVa65um43EsHRiPSjg/AnrO
dQDO4meBm7uFdqS4Gf0=
-----END CERTIFICATE-----
```

show ntp status

Displays the current active NTP server IP address or LOCL (for local switch time when no NTP servers were configured or no reachable NTP servers are available).

Syntax

show ntp status [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the active NTP server. If an NTP server is not configured, the command output displays the server as "LOCL". Otherwise, the command displays the NTP server IP address.

If the RBridge ID is not provided, status results default to the local switch (LOCL). If **rbridge-id all** is specified, the command displays the status for all switches in the cluster.

Examples

To show the local switch NTP status when an NTP server is not configured:

```
switch# show ntp status

rbridge-id 1: active ntp server is LOCL
```

To show the configured NTP server:

```
switch# show ntp status

active ntp server is 10.31.2.81
```

Related Commands

ntp server

show overlapping-vlan-resource usage

Shows the utilization of the hardware table entries that support classified or transport VLAN classifications that use overlapping C-TAGs in a Virtual Fabrics context.

Syntax

show overlapping-vlan-resource usage

Modes

Privileged EXEC mode

Usage Guidelines

This command is platform-specific. For platforms that do not have such a table for classified or TLS VLANs, the percentage is zero.

Examples

```
switch# show overlapping-vlan-resource usage
Number of table entries used:6.11%(max 4028, used 246)
```

show overlay-gateway

Displays status and statistics for the VXLAN overlay-gateway instance.

Syntax

show overlay-gateway [**name** *name* [**vlan statistics**]] [**rbridge-id** *rbridge-id*] [**statistics**]

Parameters

name

Name of the configured VXLAN gateway. Network OS supports only one gateway instance.

vlan statistics

Displays statistics for each VLAN for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts exchanged for each exported VLAN. Because each exported VLAN maps to a VXLAN, these statistics apply on a per-VXLAN-counters basis. Per-VLAN counters are not enabled by default. You need to first run the **enable statistics direction** command for the gateway to enable statistics for specified VLAN IDs.

rbridge-id *rbridge-id*

Specifies an RBridge ID.

statistics

Displays statistics for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts. These counters are derived by aggregating tunnel counters for all the tunnels of the gateway.

Modes

Privileged EXEC mode

Usage Guidelines

Output includes the gateway name, the system-assigned gateway ID, source IP address, VRF, administration state, number of tunnels associated, and the Rbridge IDs on which the gateway is configured.

This command is available only for a switch that is in logical chassis cluster mode.

If you specify the gateway name, the gateway must already be configured.

Examples

To show the status for a gateway instance that is configured for an NSX Controller:

```
switch# show overlay-gateway
Overlay Gateway "gateway1", ID 1, rbridge-ids 22-23
Type nsx, Admin state up, Tunnel mode VXLAN
IP address 10.10.10.1 ( ve1000, Vrid 100 ), Vrf default-vrf
Number of tunnels 2
Packet count: RX 0                TX 0
Byte count  : RX (NA)             TX 0
```

To show the status for a gateway instance that is configured for Layer 2 extension with a loopback interface:

```
switch# show overlay-gateway
Overlay Gateway "gateway1", ID 1, rbridge-ids 22-23
Type layer2-extension, Admin state up
IP address 10.10.10.1 (Loopback 10), Vrf default-vrf
Number of tunnels 2
Packet count: RX 0               TX 0
Byte count  : RX (NA)            TX 0
```

To show statistics for the gateway instance:

```
switch# show overlay-gateway statistics
Gateway Name         RX packets      TX packets      RX bytes        TX bytes
==================== =============== =============== ========= ==============
GW1                  200000          10000           22227772        1110111
```

To display statistics for VLANs attached to the VXLAN gateway:

```
switch# show overlay-gateway name GW1 vlan statistics
                             Packets          Bytes
VLAN    VNI     Tx      Rx        Tx         Rx
-----------------------------------------------------
10      1010   10000   200000    1110111    22227772
11      1011   2200    -         221334     -
21      1021   -       1         -          100


sw0# show overlay-gateway name test vlan statistics
VLAN ID   RX packets           TX packets
========= =================== ===================
30        0                   0
40        3696                3696
```

show policymap

Displays configured policy-maps and class-map Policer parameters applied to switch interfaces.

Syntax

show policymap [**interface** *<N>***gigabitethernet** *rbridge-id/slot/port* **input** | **output**] [**details** *policyname*]

Parameters

interface tengigabitethernet *rbridge-id/slot/port*

Interface where policy-map is bound.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

input | **output**

Direction (inbound or outbound) where the policy-map is applied.

details *policyname*

Displays the detail configuration of the policy-map along with binding information.

Modes

Global configuration mode

Interface subtype configuration mode

Usage Guidelines

Enter **show policymap** for a specific interface to display the policy-map binding settings (policy-map name and traffic direction), police-priority-map applied, and class-map Policer parameters applied for that interface.

Enter **show policymap** without identifying an interface and direction of traffic to display policy-map binding for all interfaces on the switch.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

The following are definitions of terms used in output from the **show policymap** command:

- Interface: The interface for which rate limiting information is being displayed.

- Direction: The traffic direction for which rate limiting is applied.
- police-priority-map: Remarked priority-map used for Policer application (802.1 p priority remarked map).
- Conform: The traffic in bytes that has been forwarded from this interface that is within the CIR bandwidth limits.
- Exceeded: The traffic that has been exceeded the bandwidth available in the CIR limits and has not exceed the EIR limits for this rate-limit policy.
- Violated: The traffic that has exceeded the bandwidth available in the CIR and EIR limits.
- set-dscp: The DSCP value which is applied to the traffic for the given color (conform, exceed, violate).
- set-tc: The remapped traffic class queue for the traffic for the given color (conform, exceed, violate).
- Total: The total traffic in bytes carried on this interface for the defined rate-limit policy.

Examples

To display policy-map binding and class-map parameters applied to a specific interface:

```
switch# show policymap interface tengigabitethernet 4/1 input
Interface : Ten Gigabit Ethernet 4/1
Policymap: policymapA-1
Direction: Input
Input Excluded lossless priorities: None

Class-map: default
    Police:
        cir 5 bps cbs 5678 bytes eir 512000 bps ebs 4096 bytes
        Police-priority-map: po-pr-map1
        Conformed: 30720 bytes set-dscp 0 set-tc 0
        Exceeded: 23424 bytes set-dscp 0 set-tc 0
        Violated: 0 bytes
        Total: 54144 bytes
```

To display policy-map binding information for all switch interfaces:

```
switch# show policymap
Interface : Ten Gigabit Ethernet 4/2
Inbound policy map is policymapA-1
Outbound policy map is not set
Interface : Ten Gigabit Ethernet 4/3
Inbound policy map is not set
Outbound policy map is not set
Interface : Ten Gigabit Ethernet 4/4
Inbound policy map is not set
Outbound policy map is not set
```

Related Commands

class, policy-map, qos cos, show running-config policy-map, show running-config class-map

show port port-channel

Displays the detailed LACP attributes that are configured and negotiated with its partner.

Syntax

show port port-channel *port_id*

Parameters

port_id

Port to display. The number of available channels range from 1 through 6144.

Modes

Privileged EXEC mode

show port-channel

Displays the Link Aggregation Group (LAG) information for a port-channel.

Syntax

show port-channel [*channel-group-number* | **detail** | **load-balance** | **summary**]

Parameters

channel-group-number
: Specifies a LAG port channel-group number to display. The number of available channels range from 1 through 6144.

detail
: Displays detailed LAG information for a port-channel.

load-balance
: Displays the load-balance or frame-distribution scheme among ports in the port-channel.

summary
: Displays the summary information per channel-group.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the LAGs present on the system with details about the LACP counters on their member links. LAG interfaces are called port-channels.

If you do not specify a port-channel, all port-channels are displayed.

When using the **show port-channel** *channel-group-number* command, an asterisk in the command output designates that the designated port channel is the primary link through which the BUM (Broadcast, Unknown unicast and Multicast) traffic flows.

Examples

To display detailed port-channel information:

```
switch# show port-channel detail

 LACP Aggregator: Po 10 (vLAG)(Defaulted)
 Aggregator type: Standard
 Ignore-split is enabled
 Member rbridges:
 rbridge-id: 1 (2)
 rbridge-id: 2 (1)
 Actor System ID - 0x8000,01-e0-52-00-00-01
 Admin Key: 0010 - Oper Key 0010
 Receive link count: 1 - Transmit link count: 1
 Individual: 0 - Ready: 1
 Partner System ID - 0x8000,00-05-1e-cd-0f-ea
 Partner Oper Key 0010
 Member ports on rbridge-id 2:
 Link: Te 2/0/7 (0x218038006) sync: 1
```

show port-channel-redundancy-group

Displays the port-channel redundancy-group information.

Syntax

show port-channel-redundancy-group *group-id*

Parameters

group-id

Designates which port-channel to display.

Modes

Privileged EXEC mode

Examples

Typical command execution example:

```
switch#show port-channel-redundancy-group 1
Group ID                      : 1
Member Ports                  : Port-channel 5, Port-channel 7
Configured Active Port-channel: Port-channel 5
Current Active Port-channel   : Port-channel 5
Backup Port-channel           : Port-channel 7
```

Typical command output, when the backup vLAG is operationally down or not yet created.

```
switch#show port-channel-redundancy-group 1
Group ID : 1
Member Ports                  : Port-channel 5, Port-channel 7
Configured Active Port-channel: Port-channel 5
Current Active Port-channel   : Port-channel 5
Backup Port-channel           : None
```

Typical command output, when both vLAG members are operationally down.

```
switch#show port-channel-redundancy-group 1
Group ID                      : 1
Member Ports                  : Port-channel 5, Port-channel 7
Configured Active Port-channel: Port-channel 5
Current Active Port-channel   : None
Backup Port-channel           : None
```

Typical command output, when the active vLAG is not configured.

```
switch#show port-channel-redundancy-group 1
Group ID                      : 1
Member Ports                  : Port-channel 5, Port-channel 7
Configured Active Port-channel: None
Current Active Port-channel   : Port-channel 5
Backup Port-channel           : Port-channel 7
```

show port-profile

Displays the AMPP port-profile configuration information.

Syntax

show port-profile

Modes

Privileged EXEC mode

Examples

Example of this command:

```
switch# show port-profile

port-profile default
ppid 0
  vlan-profile
    switchport
    switchport mode trunk
    switchport trunk allowed vlan all
port-profile auto-dvPortGroup-2
ppid 1
  vlan-profile
    switchport
    switchport mode trunk
    switchport trunk allowed vlan add 45
port-profile auto-dvPortGroup-1
ppid 2
  vlan-profile
    switchport
    switchport mode trunk
    switchport trunk allowed vlan add 3-10
```

Related Commands

show running-config, show port-profile interface

show port-profile domain

Displays the status of Automatic Migration of Port Profiles (AMPP) profiles and port-profile domains.

Syntax

show port-profile [*port-profile-name*] | **domain** *port-profile-domain-name*] [**status** | **activated** | **applied**] | **associated**]

Parameters

port-profile-name
The name of a port-profile.

domain
Enables specification of a port-profile domain name.

port-profile-domain-name
Name of a port-profile domain.

status
Enables selection of status type.

activated
Specifies all port-profiles with the activated status.

applied
Specifies all port-profiles with the applied status.

associated
Specifies all port-profiles with the associated status.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **show port-profile status** to display the status of all AMPP profiles.

If **no** option is specified, then all port-profiles that match the criteria are shown.

Examples

The following example shows the status of all port-profiles:

```
switch# show port-profile status
Port-Profile        PPID   Activated    Associated MAC     Interface
auto-dvPortGroup-2   1      Yes          0050.5681.2ed5      none

                                                          0050.5699.5524      te0/2

                                                          0050.5699.39e0      te0/1
auto-dvPortGroup-1   2      Yes          0050.5681.083c      none
```

The following example shows the status of a port-profile domain:

```
switch# show port-profile domain vDC1_Domain status
Port-Profile  PPID   Activated   Associated MAC   Interface
Tenant1_PP     1      No           None             None
Tenant2_PP     2      No           None             None
```

Related Commands

show running-config, show running-config port-profile-domain, show port-profile, show port-profile interface

show port-profile interface

Displays AMPP port-profile information for interfaces.

Syntax

show port-profile interface [**all** | **port-channel** *channel-group-number* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

all

Displays the port-profile information for all interfaces.

port-channel *channel-group-number*

Specifies a LAG port channel-group number to display. Valid values range from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display AMPP port-profile information for either all interfaces, or for specific interfaces.

Related Commands

show running-config, show port-profile

show port-profile name

Displays the port profile information for a named port-profile.

Syntax

show port-profile name *port-profile-name* { **qos** | **security** | **status** | **vlan** }

show port-profile name *port-profile-name* **name** *port-profile-name* **validate**

Parameters

port-profile-name

The name of the port-profile. The maximum number of characters is 64.

qos

QoS sub-profile

security

Security sub-profile

status

Specific port-profile status

vlan

VLAN sub-profile

validate

Validates two port-profiles against each other.

Modes

Privileged EXEC mode

show port-security

Displays the configuration information related to port security.

Syntax

show port-security

Modes

Privileged EXEC mode

Examples

```
switch# show port-security
Secure  MaxSecureAddr      CurrentAddr      StaticSec  Violated     Action      OUIs     Sticky
Port       (count)       (count)     (count)
Te 1/1      2                 1               3             No           Restrict     2       No
Te 1/3      3                 3               5             Yes          Shutdown     0       Yes
```

show port-security addresses

Displays the configuration information related to port-security addresses.

Syntax

show port-security addresses

Modes

Privileged EXEC mode

Examples

```
switch# show port-security addresses
                    Secure Mac Address Table
------------------------------------------------------------------
Vlan                Mac Address      Type                 Ports
1                 0000.0000.0001       Secure-Dynamic       1/1
1                 0000.0000.0002       Secure-Static        1/2
```

show port-security interface

Displays the configuration information related to port-security interfaces.

Syntax

show port-security interface [**all** | **port-channel** *channel-group-number* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

all

Displays the port-security information for all interfaces.

port-channel *channel-group-number*

Specifies a LAG port channel-group number to display. Valid values range from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show port-security interface TenGigabitEthernet 1/1
Port Security              :Enabled
Port Status                :up / Down (Security Violated)
Violation Mode             :Restrict
Violated                   :Yes/No
Sticky enabled             :Yes/No
Maximum MAC Addresses      :2
Total MAC Addresses        :2
Configured MAC Addresses   :5
Violation time       : Fri Mar 22 05:53:03 UTC 2013
Shutdown time(in Minutes)  :5
Number of OUIs configured  :1
```

show port-security oui interface

Displays the configuration information related to port security for Organizationally Unique Identifier (OUI) interfaces.

Syntax

show port-security oui interface

Modes

Privileged EXEC mode

Examples

```
switch# show port-security oui interface TenGigabitEthernet 1/1
OUIs configured             : 3
OUIs                        : 0010.0a00.0000
                              0020.0b00.0000
                              0030.0c00.0000
```

show port-security sticky interface

Displays the configuration information related to port security for a sticky interface.

Syntax

show port-security sticky interface

Modes

Privileged EXEC mode

Examples

```
switch# show port-security sticky interface TenGigabitEthernet 1/1
VlanId   Mac-address       Type             State        Ports
1        0000.0000.1111    Secure-Sticky    Active       Te 1/1
```

show process cpu

Displays information about the active processes in the switch and their corresponding CPU utilization statistics.

Syntax

show process cpu [**rbridge-id** { *rbridge-id* | **all** }] [**summary**] [**history**] [**top**]

Parameters

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

summary
Displays a summary view of cpu usage.

history
Displays the history of CPU usage.

top
Displays current CPU utilization.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

For an explanation of process states, refer to the UNIX manual page for the **ps** command.

Examples

To show the information for all processes:

```
switch# show process cpu summary

Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.03; Fifteen minutes: 0.01
```

To show CPU usage information by individual processes:

```
switch# show process cpu

Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.02; Fifteen minutes: 0.00
Active Processes Lifetime Statistic:
  PID   Process          CPU%  State      Started
17169   sh                1.00    S       13:44:27 Jul  1, 2012
 2060   emd               0.80    S       21:52:27 Jun 29, 2012
 2462   SWITCH_TMR_0      0.60    S       21:53:08 Jun 29, 2012
17170   imishow_proc_cp   0.50    S       13:44:27 Jul  1, 2012
 2207   ospfd             0.20    S       21:52:41 Jun 29, 2012
 2211   mstpd             0.20    S       21:52:41 Jun 29, 2012
 2208   rtmd              0.10    S       21:52:41 Jun 29, 2012
(Output truncated)
```

Related Commands

show process memory, show process info

show process info

Displays system processes hierarchically.

Syntax

show process info [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

This command is executed on the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Pagination is not supported with this command. Use **more** in the terminal window to display the output one page at a time.

This command is supported only on the local switch.

Examples

To display system processes hierarchically:

```
switch# show process info

PID     CMD
2       kthreadd
3       \_ migration/0
4       \_ ksoftirqd/0
5       \_ watchdog/0
6       \_ migration/1
7       \_ ksoftirqd/1
8       \_ watchdog/1
9       \_ migration/2
10      \_ ksoftirqd/2
11      \_ watchdog/2
12      \_ migration/3
13      \_ ksoftirqd/3
14      \_ watchdog/3
15      \_ migration/4
16      \_ ksoftirqd/4
17      \_ watchdog/4
18      \_ migration/5
19      \_ ksoftirqd/5
20      \_ watchdog/5
21      \_ migration/6
22      \_ ksoftirqd/6
(Output truncated)
```

Related Commands

show process cpu, show process memory

show process memory

Displays the memory usage information based on processes running in the system.

Syntax

show process memory [**rbridge-id** { *rbridge-id* | **all** }] [**summary**]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

summary

Displays a summary view of memory usage.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To show memory usage information by individual processes:

```
switch# show process memory

Rbridge-id: 54
%Memory Used: 48.9778%; TotalMemory: 3354812 KB; Total Used: 1643112 KB
Total Free: 1711700 KB; Low Free: 759700 KB; High Free: 500156 KB; Cached: 406696 KB
  PID   Process          MEM%        VSIZE(KB)       RSS(KB)        PSS(KB)
 2895   postgres         4.30         203788         147224         101079
 2682   Dcmd.Linux.powe  4.30         324416         145956         119904
 3063   ospf6d           2.80         375424          94816          51118
 3042   rps              2.70         266576          93800          73916
 2890   postgres         2.60         155492          89616          46558
 3039   ospfd            2.50         367280          86068          42306
 3038   bgpd             2.40         372888          81520          37625
 3050   vrrpd            1.90         289480          65700          21929
 3040   ribmgr           1.90         203156          65004          45139
 4370   fibagt           1.60         184816          55772          36110
 3041   srm              1.60         183608          54272          34579
 3044   pimd             1.50         288724          53040          33215
 1264   confd            1.40          58856          46984          45873
 2336   raslogd          1.30         192276          44488          21016
 3055   iphelpd          1.30         232224          44360          24545
 3034   nsm              1.30         265352          43720          23292
 3054   arpd             1.20         209820          41276          21638
 3049   mstpd            1.10         200420          39768          19836
 3061   toamd            1.10         189932          38592          18752
 3064   tnlmgrd          1.10         181312          37580          18049
 2965   snmpd            1.00         135320          34012          11760
 3046   ssmd             0.90         179288          31504          11510
 4366   l2agtd           0.90         165984          31304          11608
 3045   mldd             0.80         184660          29948           9992
 3036   l2sysd           0.80         225680          29688           9596
 3047   qosd             0.80         175688          29068           9141
 3052   igmpd            0.80         176268          28684           8803
 3043   radv             0.80         164956          27352           7562
 4368   mcagtd           0.80         156732          27048           7351
 3056   onmd             0.70         175700          26812           6707
 3048   lacpd            0.70         166880          26280           6153
[output omitted, as will vary by device]

 3491   TD_TX_0          0.00              0              0              0
 4273   DCE_BLADE_THR_0  0.00              0              0              0
 4274   CBR_BH_43008080  0.00              0              0              0
 4275   CBR_HI_43008080  0.00              0              0              0
 4276   CBR_TX_43008080  0.00              0              0              0
 4277   CBR_RX_43008080  0.00              0              0              0
 4278   CBR_AS_43008080  0.00              0              0              0
 4279   CBR_MM_43008080  0.00              0              0              0
 4280   DCE_BLADE_CH_TH  0.00              0              0              0
 4282   FCOE_AGT_MI_THR  0.00              0              0              0
```

Related Commands

show process cpu, show process info

show prom-access

Shows the Boot PROM access status.

Syntax

show prom-access

Command Default

The boot PROM is accessible.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to determine whether the Boot PROM is accessible.

Under non-FIPS compliant operation, you can access the Boot PROM by holding down the ESC key during the 4-second period when the switch is booting up. In FIPS compliant state, PROM access is disabled to prevent users from net-installing firmware.

If PROM access is enabled, you can disable it in preparation for FIPS compliance. If PROM access is disabled, you cannot re-enable it.

Enter the **unhide fips** command with password "fibranne" to make the command available.

Examples

To view the Boot PROM access status:

```
switch# show prom-access

PROM access Enabled
```

Related Commands

cipherset, fips selftests, fips zeroize, unhide fips

show qos flowcontrol interface

Displays all of the configured flow control information for an interface.

Syntax

show qos flowcontrol interface [**<N>gigabitethernet** *rbridge-id/slot/port* | **all**]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

all

Reports QoS flow control statistics for all interfaces within the system.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the runtime state retrieved frm the dataplane reflecting the operation of 802.3x pause or Priority Flow Control (PFC) on an interface.

The administrative state for pause generation and reception or processing is presented for the interface (802.3x mode) or for each CoS (PFC mode). TX_Pause frame generation statistics are always presented for the interface. The RX_Pause BitTimes is presented for the interface (802.3x mode) or for each CoS (PFC mode). When PFC is deployed under the CEE Provisioning model, then the command reports whether the Data Center Bridging eXchange protocol (DCBX) has overridden the user configuration, for example when the DCBX detects a mis-configuration between CEE peers, it disables PFC operationally.

Examples

To display all of the configured flow control information for a 10-gigabit Ethernet interface:

```
switch# show qos flowcontrol interface tengigabitethernet 5/0/1

Interface Ten Gigabit Ethernet 5/0/1
  Mode PFC
  DCBX enabled for PFC negotiation
  TX 0 frames
         TX   TX    RX   RX Output Paused
  CoS Admin Oper Admin Oper  512 BitTimes
  ----------------------------------------
    0   Off  Off   Off  Off             0
    1   Off  Off   Off  Off             0
    2    On  Off    On  Off             0
    3   Off  Off   Off  Off             0
    4   Off  Off   Off  Off             0
    5   Off  Off   Off  Off             0
    6   Off  Off   Off  Off             0
```

Related Commands

show qos interface, show cee maps

show qos interface

Displays a summary of all QoS configurations applied on an interface.

Syntax

show qos interface [<*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **all**]

Command Default

If no interface is specified, QoS information for all interfaces is displayed.

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the port-channel of the interface. Valid values range from 1 through 63.

all

Reports QoS configurations for all interfaces within the system.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a summary of all QoS configuration applied on an interface, including QoS Provisioning mode, CEE map, Layer 2 priority, Traffic Class mapping, congestion control, and the scheduler policy.

Examples

To display all of the configured QoS information for a 10-gigabit Ethernet interface:

```
switch# show qos interface tengigabitethernet 22/0/1

Interface Ten Gigabit Ethernet 22/0/1
  Provisioning mode cee
  CEE Map demo
  Default CoS 0
  Interface trust cos
  CoS-to-CoS Mutation map 'default'
                In-CoS:   0   1   2   3   4   5   6   7
     ---------------------------------------------------
     Out-CoS/TrafficClass: 0/4 1/4 2/6 3/4 4/4 5/4 6/4 7/4
  Tail Drop Threshold 1081344 bytes
  Per-CoS Tail Drop Threshold (bytes)
          CoS:      0      1      2      3      4      5      6      7
     ------------------------------------------------------------------
     Threshold: 129761 129761 129761 129761 129761 129761 129761 129761
  Flow control mode PFC
     CoS2 TX on, RX on
  Multicast Packet Expansion Rate Limit 3000000 pkt/s, max burst 4096 pkts
  Multicast Packet Expansion Tail Drop Threshold (packets)
TrafficClass:    0    1    2    3    4    5    6    7
     ------------------------------------------------
Threshold:      64   64   64   64   64   64   64   64
  Traffic Class Scheduler configured for 0 Strict Priority queues
     TrafficClass:   0   1   2   3   4   5   6   7
     ------------------------------------------
       DWRRWeight:   0   0   0   0  60   0  40   0
  Multicast Packet Expansion Traffic Class Scheduler
TrafficClass:    0    1    2    3    4    5    6    7
     ------------------------------------------------
DWRRWeight:     25   25   25   25   25   25   25   25
```

Related Commands

cee-map (FCoE)

show qos maps

Displays information on the defined QoS maps.

Syntax

show qos maps [**cos-mutation** [*name*] | **cos-traffic-class** [*name*]]

Command Default

Report shows all defined QoS maps.

Parameters

cos-mutation *name*

Specifies to report on only the named CoS-to-CoS mutation QoS map.

cos-traffic-class *name*

Specifies to report on only the named CoS-to-Traffic Class QoS map.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information on the QoS defined maps. For each QoS map, the configuration state is displayed with a list of all interfaces bound to the QoS map.

Examples

To display information on the defined QoS maps:

```
switch# show qos maps

  CoS-to-CoS Mutation map 'test'
      In-CoS:  0  1  2  3  4  5  6  7
     ---------------------------------
     Out-CoS:  0  1  2  3  5  4  6  7
     Enabled on the following interfaces:
      Te 0/5
  CoS-to-Traffic Class map 'test'
          Out-CoS:  0  1  2  3  4  5  6  7
     ------------------------------------
     TrafficClass:  0  1  2  3  5  4  6  7
     Enabled on the following interfaces:
      Te 0/5
```

Related Commands

qos map cos-traffic-class, show qos interfaceqos map cos-traffic-class, show qos interface

show qos maps dscp-cos

Displays configured DSCP-CoS maps.

Syntax

show qos maps dscp-cos

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP-CoS maps and application on interfaces.

```
sw0# show qos maps dscp-cos

Dscp-to-CoS map 'test' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------
 0 :    00 03 07 03 07 03 07 03 07 01
 1 :    01 05 06 05 06 05 06 05 06 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 04 04 04 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 3
mark 11,13,15,17 to 5
mark 12,14,16,18 to 6
mark 2,4,6,8 to 7
```

Related Commands

qos map dscp-cos, show qos interface

show qos maps dscp-mutation

Displays configured DSCP-mutation maps.

Syntax

show qos maps dscp-mutation

Modes

Privileged EXEC mode

Usage Guidelines

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To display information on defined QoS DSCP-mutation maps.

```
sw0# show qos maps dscp-mutation

Dscp-to-Dscp Mutation map 'test' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    00 09 10 09 10 09 10 09 10 09
 1 :    10 19 20 19 20 19 20 19 20 19
 2 :    20 21 22 23 24 25 26 27 28 29
 3 :    30 31 32 33 34 35 36 37 38 39
 4 :    40 41 42 43 44 45 46 47 48 49
 5 :    50 51 52 53 54 55 56 57 58 59
 6 :    60 61 62 63
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 9
mark 11,13,15,17 to 19
mark 12,14,16,18 to 20
mark 2,4,6,8 to 10
```

Related Commands

qos map dscp-mutation

show qos maps dscp-traffic-class

Displays configured DSCP-Traffic-Class maps.

Syntax

show qos maps dscp-traffic-class

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP-Traffic-Class maps.

```
sw0# show qos maps dscp-traffic-class

Dscp-to-Dscp Mutation map 'test' (dscp= d1d2)
Dscp-to-Traffic Class map 'pqrs'(dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
---------------------------------------
 0 :    00 03 07 03 07 03 07 03 07 01
 1 :    01 05 06 05 06 05 06 05 06 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 04 04 04 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
Enabled on the following interfaces:
    Te 16/2/2
```

This information relates to the following map configuration applied to interface 16/2/2:

```
qos map dscp-mutation test
mark 1,3,5,7 to 3
mark 11,13,15,17 to 5
mark 12,14,16,18 to 6
mark 2,4,6,8 to 7
```

Related Commands

show qos interface

show qos queue interface

Displays the runtime state retrieved from the interface reflecting the number of packets and bytes sent and received for each priority.

Syntax

show qos queue interface [*<N>*gigabitethernet *rbridge-id/slot/port* | **all**]

Parameters

*<N>*gigabitethernet

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>* gigabitethernet with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

all

Reports QoS statistics for all Ethernet interfaces within the system.

Modes

Privileged EXEC mode

Examples

To display the queueing information for a 10-gigabit Ethernet interface:

```
switch# show qos queue interface tengigabitethernet 5/0/2

Interface Ten Gigabit Ethernet 5/0/2
               RX             RX                   TX             TX
  CoS      Packets          Bytes      TC      Packets          Bytes
  -------------------------------     -------------------------------
    0       680458       87098624       0            0              0
    1            0              0       1        32318              0
    2            0              0       2            0              0
    3            0              0       3            0              0
    4            0              0       4            0              0
    5            0              0       5            0              0
    6            0              0       6            0              0
    7            0              0       7            0              0
```

Related Commands

cee-map (configuration), qos map cos-mutationcee-map (configuration), qos map cos-mutation

show qos rcv-queue interface

Displays a summary of the runtime ingress queue state information applied to a Layer 2 interface.

Syntax

show qos rcv-queue interface [*<N>***gigabitethernet** *rbridge-id/slot/port* | **all**]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

all

Reports QoS configurations for all 10-gigabit Ethernet interfaces within the system.

Modes

Privileged EXEC mode

Usage Guidelines

This command is not supported on Brocade VDX 8770-4 and VDX 8770-8 platforms.

Examples

To display the runtime ingress queue state information retrieved from the dataplane for a 10-gigabit Ethernet interface:

```
switch# show qos rcv-queue interface tengigabitethernet 22/0/2

Interface TenGigabitEthernet 22/0/2
  In-use 404019 bytes, Max buffer 1081344 bytes
  0 packets dropped
          In-use        Max
  CoS      Bytes      Bytes
  ------------------------
    0          0    1081344
    1          0    1081344
    2     404019    1081344
    3          0    1081344
    4          0    1081344
    5          0    1081344
    6          0    1081344
    7          0    1081344
```

Related Commands

show qos rcv-queue multicast

show qos rcv-queue multicast

Displays the runtime state retrieved from the dataplane reflecting any multicast packet expansion packet drops resulting from a queue crossing the maximum queue depth.

Syntax

show qos rcv-queue multicast [*<N>***gigabitethernet** *rbridge-id/slot/port* | **all**]

Parameters

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

all

Reports QoS multicast packet expansion receive queueing statistics for all ASICs within the system.

Modes

Privileged EXEC mode

Usage Guidelines

This command is not supported on Brocade VDX 8770-4 and VDX 8770-8 switches.

Examples

To display the queueing information:

```
switch# show qos rcv-queue multicast tengigabitethernet 1/0/2

Dropped Counts
  Linecard/Portset           TC 0           TC 1           TC 2           TC 3
--------------------------------------------------------------------------------
         0/0                    0              0              0              0
```

Related Commands

show qos rcv-queue interface

show qos red profiles

Displays configured Random Early Discard (RED) profiles.

Syntax

show qos red profiles

Modes

Privileged EXEC mode

Usage Guidelines

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

Using **show qos red profiles** to display information on defined QoS RED profiles:

NOTE
Notice that the first example shows output for the RED profile configured in the example for the **qos red profile** command.

```
switch# show qos red profiles

Red Profile 2
        Minimum Threshold: 10
        Maximum Threshold: 80
        Drop Probability: 80
Activated on the following interfaces:
Te 1/2/2  Traffic-class: 7
Red Profile 100
        Minimum Threshold: 30
        Maximum Threshold: 80
        Drop Probability: 56
Activated on the following interfaces:
Te 1/1  Traffic-class: 2
Red Profile 200
        Minimum Threshold: 40
        Maximum Threshold: 60
        Drop Probability: 40
Activated on the following interfaces:
Te 1/1  Traffic-class: 4
```

Using **show qos interface** *interface-name* to examine the applied RED profiles for a specific interface:

```
switch# show qos interface te 1/2/2

Interface Ten Gigabit Ethernet 1/2/2
  Provisioning mode non-cee
  Default CoS 0
  Interface COS trust untrusted
  CoS-to-CoS Mutation map 'default'
  CoS-to-Traffic Class map 'default'
                  In-CoS:   0   1   2   3   4   5   6   7
     ---------------------------------------------------
     Out-CoS/TrafficClass: 0/1 0/1 0/1 0/1 0/1 0/1 0/1 0/7
  Interface DSCP trust untrusted
  DSCP-to-DSCP Mutation map 'default' (dscp= d1d2)
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
  ------------------------------------
   0 :    00 01 02 03 04 05 06 07 08 09
   1 :    10 11 12 13 14 15 16 17 18 19
   2 :    20 21 22 23 24 25 26 27 28 29
   3 :    30 31 32 33 34 35 36 37 38 39
   4 :    40 41 42 43 44 45 46 47 48 49
   5 :    50 51 52 53 54 55 56 57 58 59
   6 :    60 61 62 63
  RED Enabled on the following Priorities:
        CoS: 7, Profile: 2
more
```

Related Commands

qos red profile

show qos red statistics interface

Displays Random Early Discard (RED) statistics for a specific interface.

Syntax

show qos red statistics interface *interface-name*

Parameters

interface-name

Name of interface where an RED profile is applied.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display statistics for RED on a specific interface where a RED profile is applied. Statistics include packets and bytes dropped for the CoS priority mapped to the profile for the interface.

Examples

To display RED statistics on interfaces, use the **show qos red statistics interface** *interface-name* command. Notice that the colors in the following example (red, yellow, and green) relate to color-based priority mapping set through the Port-Based Policer feature. Refer to the *Network OS Administrator's Guide* for more information.

```
switch# show qos red statistics interface te 2/1

Statistics for interface: Te 2/1
Traffic-class: 2, ProfileId: 20
Packets Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
Bytes Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
Traffic-class: 3, ProfileId: 10
Packets Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
Bytes Dropped: Red: 0,  Yellow: 0, Green: 0, Queue Drops: 0
```

Related Commands

qos red profile, show qos red profiles

show qos tx-queue interface

Displays a summary of the runtime egress queue state information applied to a Layer 2 interface.

Syntax

show qos tx-queue interface [*<N>***gigabitethernet** *rbridge-id/slot/port* | **all**]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

all

Reports QoS configurations for all 10-gigabit Ethernet interfaces within the system.

Modes

Privileged EXEC mode

Usage Guidelines

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on the Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

To display the runtime egress queue state information retrieved from the dataplane for a tengigabit Ethernet interface:

```
switch# show qos tx-queue interface tengigabitethernet 1/0/7
Interface TenGigabitEthernet 1/0/7 Transmit Queues
  In-use 0 bytes, Max buffer 5046272 bytes
  0 packets dropped
          In-use        Max
  TC       Bytes      Bytes
  ------------------------
    0          0     630784
    1          0     630784
    2          0     630784
    3          0     630784
    4          0     630784
    5          0     630784
    6          0     630784
    7          0     630784
```

History

Release version	Command history
5.0.0	This command was introduced.

show rbridge-id

Displays the RBridge ID of each node that is configured in a Virtual Cluster Switching (VCS) cluster.

Syntax

show rbridge-id [**swbd-number** *int* | **chassis** { **virtual-ip** }

Parameters

swbd-number

Selects a switch type.

int

One or more integers (including a decimal) that identifies a switch type.

chassis virtual-ip

Displays virtual IP addresses if configured

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view the RBridge IDs of configured nodes in a VCS cluster, in addition to the switch type (SWBD) number and IPv4 and IPv6 virtual IP addresses.

Examples

```
switch# show rbridge-id
RBRIDGE  SWBD
ID       NUMBER  V4  V6
-------------------------
154      95      -   -
```

Related Commands

rbridge-id

show rbridge-running config

Displays the currently running configuration for an RBridge.

Syntax

show rbridge-running-config rbridge-id *rbridge-id*

Parameters

rbridge-id *rbridge-id*

Specifies the RBridge ID whose configuration will be displayed.

Modes

Privileged EXEC mode

Examples

The following example shows partial output for this command:

```
switch# show rbridge-running-config rbridge-id 1
diag post rbridge-id 1
 enable
!
dpod 1/0/1
 reserve
!
dpod 1/0/2
 reserve
!
dpod 1/0/3
 reserve
!
dpod 1/0/4
!
dpod 1/0/5
!
dpod 1/0/6
!
dpod 1/0/7
!
[output truncated for brevity]

logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 1
 chassis-name VDX6720-24
 host-name rb1
```

Related Commands

show global-running-config, show rbridge-local-running-config

show rbridge-local-running-config

Displays the current local configuration for an RBridge.

Syntax

show rbridge-local-running-config [**rbridge-id** *rbridge-id*]

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

The following example shows partial output for this command:

```
switch# show rbridge-local-running-config rbridge-id 1
diag post rbridge-id 1
 enable
!
dpod 1/0/1
 reserve
!
dpod 1/0/2
 reserve
!
dpod 1/0/3
 reserve
!
dpod 1/0/4
!
dpod 1/0/5
!
dpod 1/0/6
!
dpod 1/0/7
!
dpod 1/0/8
!
dpod 1/0/9
!
dpod 1/0/10
!
dpod 1/0/11
!
dpod 1/0/12
!
dpod 1/0/13
!
dpod 1/0/14
!
dpod 1/0/15
!
dpod 1/0/16
!
dpod 1/0/17
!
dpod 1/0/18
!
dpod 1/0/19
!
dpod 1/0/20
!
dpod 1/0/21
!
dpod 1/0/22
!
dpod 1/0/23
!
dpod 1/0/24
!

switch-attributes 1
 chassis-name VDX6720-24
 host-name rb1
!
fabric route mcast rbridge-id 1
!
rbridge-id 1
 ip route 0.0.0.0/0 10.17.0.1
 switch-attributes chassis-name VDX6720-24
 switch-attributes host-name rb1
 system-monitor fan threshold marginal-threshold 1 down-threshold 2
```

```
 system-monitor fan alert state removed action raslog
 system-monitor power threshold marginal-threshold 1 down-threshold 2
 system-monitor power alert state removed action raslog
 system-monitor temp threshold marginal-threshold 1 down-threshold 2
 system-monitor cid-card threshold marginal-threshold 1 down-threshold 2
 system-monitor cid-card alert state none action none
 system-monitor sfp alert state none action none
 system-monitor compact-flash threshold marginal-threshold 1 down-threshold 0
 system-monitor MM threshold marginal-threshold 1 down-threshold 0
 system-monitor LineCard threshold marginal-threshold 1 down-threshold 2
 system-monitor LineCard alert state none action none
 system-monitor SFM threshold marginal-threshold 1 down-threshold 2
 no protocol vrrp
 no protocol vrrp-extended
 interface Ve 123
  shutdown
 !

!
interface Management 1/0
 no ip address dhcp
 ip address 10.17.10.21/20
 ip gateway-address 10.17.0.1
 no ipv6 address autoconfig
 no ipv6 address dhcp
!
interface TenGigabitEthernet 1/0/1
 description LC 1/0/1-23
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 1/0/2
 description LC 1/0/1-23
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 1/0/3
 mtu 9216
 description LC 1/0/1-23
 fabric isl enable
 fabric trunk enable
 switchport
 switchport mode access
 switchport access vlan 1
 no shutdown
!
interface TenGigabitEthernet 1/0/4
 mtu 9216
 description LC 1/0/1-23
```

Related Commands

show global-running-config, show rbridge-running config

show redundancy

Displays the control processor redundancy settings of the Management Module (MM).

Syntax

show redundancy

Modes

Privileged EXEC mode

Examples

To show redundancy:

```
switch# show redundancy
=== MM Redundancy Statistics ===
Current Active Session:
Active Slot = M2 (Local), Failover Cause: Failed Over
Standby Slot = M1 (Remote)
Start Time: 11:11:08 UTC Wed Nov 28 2012
Previous Active Session:
Active Slot = M1
Standby Slot = M2
End Time: 09:50:07 UTC Wed Nov 28 2012
System Uptime: 09:42:12 UTC Wed Nov 28 2012
```

Related Commands

ha enable, ha failover, show ha

show rmon

Displays the current RMON status on the switch.

Syntax

show rmon [**alarms** [*number*] [**brief**] | **events** [*number*] [**brief**] | **logs** [*event_number*] | **statistics** [*number*] [**brief**]]

Parameters

alarms

Specifies to display the RMON alarm table.

number

Specifies the alarm index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

events

Specifies to display the RMON events table.

number

Specifies the event index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

logs

Specifies to display the RMON log table.

event_number

Specifies the event log index identification number. Valid values range from 1 through 65535.

statistics

Specifies to display the statistics identification number.

number

Specifies the statistics identification number. Valid values range from 1 through 65535.

brief

Specifies a brief summary of the output.

Modes

Privileged EXEC mode

Examples

To display the RMON statistics:

```
switch# show rmon statistics

rmon collection index 4
    Interface index is Id: 67108864 , Name : Ten Gigabit Ethernet 0/0
    Receive Statistics:
        218903 packets, 14015626 bytes,  0 packs dropped
        Multicasts: 218884, Broadcasts: 18
        Under-size : 0, Jabbers: 0, CRC: 0
        Fragments: 0, Collisions: 0
             64 byte pkts: 218722, 65-127 byte pkts: 174
        128-255 byte pkts: 0, 256-511 byte pkts: 6
        512-1023 byte pkts: 0, 1024-1518 byte pkts: 0
        Over 1518-byte pkts(Oversize - Jumbo): 0
    Owner: RMON_SNMP
    Status: ok(1)
```

To display the RMON events:

```
switch# show rmon events

event Index = 4
        Description "My Description"
        Event type Log & SnmpTrap
        Event community name admin
        Last Time Sent = 00:00:00
        Owner  admin
```

Related Commands

rmon alarm, rmon event

show rmon history

Displays information gathered by rmon event and rmon alarm commands.

Syntax

show rmon history [**statistics** | *history_index*]

Parameters

statistics

Displays a more detailed synopsis.

history_index

Specifies the RMON history identification number. Valid values range from 1 through 65535.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a synopsis of the statistics collected by the **rmon event** and **rmon alarm** commands.

Add the **statistics** parameter to display the detailed history.

Examples

To display the RMON history:

```
switch# show rmon history

RMON history control entry 1
interface: ifIndex.1745682445 Ten Gigabit Ethernet 0/13
buckets requested: 20
buckets granted: 20
sampling interval: 10
Owner: jsmith
```

Related Commands

rmon alarm, rmon event

show route-map

Displays all interfaces in the system that currently have a route map applied.

Syntax

show route-map [*name*] [**rbridge-id** { *rbridge-id* | **all** }]

show route-map ve *vlan-id* { **rbridge-id** *rbridge-id* | **all**] }

Parameters

name
The name of the route-map.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

ve *vlan_id*
Specifies the interface Ve for specified RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Output indicators are as follows:

- Active/Partial/Inactive status: Indicates the instantiation of the route-map configuration into the underlying hardware. Possible meanings for inactive may be no room in the TCAM for programming the ACL, or the exhaustion of next-hop entries within the hardware next-hop table.
- Selected: Indicates which of the configured next hops is currently being used by the policy. If the keyword selected is absent from the display, it indicates that none of the next hops in the list is being used and the packet is being routed by the standard routing mechanism.
- Count: Provides a summary of the number of times any of the match criteria within the specific ACL has been hit. If the ACL binding was unable to allocate a counter for the ACL (due to resource exhaustion), the count value will show "Counter not available." Otherwise, an actual counter value is displayed.

Examples

```
sw0# show route-map
Interface TenGigabitEthernet 3/3
   Ip Policy Route-map abc
Interface TenGigabitEthernet 3/4
   Ip Policy Route-map bar
```

Example of **show route-map** by application:

```
sw0# show route-map abc
Interface TenGigabitEthernet 3/3
  ip policy route-map abc permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip precedence critical
    set ip next-hop 3.3.1.1  (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes
ip policy route-map abc permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip precedence flash
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
    set ip interface null0
    Policy routing matches: 0 packets; 0 bytes
sw0# show route-map xyz
Interface TenGigabitEthernet 3/4
  ip policy route-map xyz deny 10 (inactive)
    match ip address acl Vincent
    set ip precedence critical
    set ip vrf pulp_fiction next-hop 3.3.3.5  (selected)
    set ip next-hop 4.4.4.4
    Policy routing matches: Counter not available
sw0# show route-map abc rbridge-id all
Interface TenGigabitEthernet 204/3/3
  ip policy route-map abc permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip next-hop 3.3.1.1  (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes
Interface Ve 3 on rbridge-id 205
  ip policy route-map abc permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
    set ip interface null0
    Policy routing matches: 0 packets; 0 bytes
```

Related Commands

ip policy route-map

show route-map interface

Displays the status of a route-map application on the specified interface.

Syntax

show route-map interface { **port-channel** *index* | *<N>***gigabitethernet** *slot/port* | **ve** *vlan-id* }

show route-map interface ve *vlan-id* **rbridge-id** { *rbridge-id* | **all** }

Parameters

port-channel *index*

Displays the status of the port-channel interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port

Specifies a valid port number.

ve *vlan-id*

Displays the status of a route-map application on the specified virtual Ethernet interface Ve for the mentioned rbridge-id.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

You do not need to specify the route map name, as only a single route map can be applied to an interface.

Examples

To display the status of a route map on a 10-gigabit Ethernet interface:

```
sw0# show route-map interface tengigabitethernet 3/3
Interface TenGigabitEthernet 3/3
  ip policy route-map foo permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip next-hop 3.3.1.1  (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes
  ip policy route-map foo permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
    set ip interface null0
    Policy routing matches: 0 packets; 0 bytes
sw0# show route-map interface Ve 3 rbridge-id all
Interface Ve 3 on rbridge-id 205
  ip policy route-map foo permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip precedence critical
    set ip next-hop 3.3.1.1  (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes
Interface Ve 3 on rbridge-id 206
  ip policy route-map foo permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
    set ip interface null0
    Policy routing matches: 0 packets; 0 bytes
```

Related Commands

ip policy route-map

show running reserved-vlan

Displays the range of reserved VLAN values.

Syntax

show running reserved-vlan

Modes

Privileged EXEC mode

Related Commands

reserved-vlan, show default-vlan

show running-config

Displays the contents of the running configuration.

Syntax

show running-config

Parameters

Refer to the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the running configuration. This is the configuration that is currently active on the local switch but which is not saved persistently.

This command is supported only on the local switch.

Enter **show running-config ?** to display the list of available configuration entries.

Examples

To display the running configuration:

```
switch# show running-config

chassis virtual-ip 10.24.73.50/20
no diag post enable
linecard 2 LC48x10G
linecard 4 LC48x10G
class-map default
 match any
!
logging rbridge-id 1
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 1
 chassis-name VDX8770-4
 host-name sw0
!
support rbridge-id 1
 ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common!
(Output truncated)
```

Related Commands

show startup-config, show startup-db

show running-config aaa

Displays the configuration attributes for the authentication, authorization, and accounting (AAA) server from the configuration database.

Syntax

show running-config aaa [**accounting** [**commands** | **exec**] | **authentication** [**login**]]

Parameters

accounting

Configures Login or Command accounting

commands

Enable/Disable Command accounting

exec

Enable/Disable Login accounting

authentication

Configures preferred order of Authentication output modifiers

login

Configures the order of sources for login (default = 'local')

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To display the authentication mode:

```
switch# show running-config aaa
aaa authentication radius local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none

switch# show running-config aaa authentication
aaa authentication login radius local

switch# show running-config aaa authentication
aaa authentication login ldap local-auth-fallback
```

Related Commands

aaa authentication

show running-config aaa accounting

Displays the AAA server accounting configuration.

Syntax

show running-config aaa accounting

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To displaying the authentication mode:

```
switch# show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

Related Commands

aaa authentication

show running-config access-list

Displays a list of ACLs defined on the switch, including the rules they contain.

Syntax

show running-config ip access-list [**standard** | **extended**] [*ACL_name*]

show running-config ipv6 access-list [**standard** | **extended**] [*ACL_name*]

show running-config mac access-list [**standard** | **extended**] [*ACL_name*]

Parameters

standard | **extended**

Specifies the ACL type. Not specifying the ACL type displays all standard and extended ACLs of the given type.

ACL_name

Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

To display details of ACLs bound to interfaces, use the **show access-list** command.

Examples

The following example displays all IPv4 ACLs in the running-config of the local switch:

```
switch# show running-config ip access-list
ip access-list extended ip1
 seq 10 permit ip host 192.168.100.2 any
!
ip access-list extended ip_1
 seq 10 permit ip any host 172.10.15.200 count
!
ip access-list extended ip_2
 seq 10 permit ip any host 172.10.16.200 count
!
ip access-list extended ip_3
 seq 10 permit ip host 172.10.16.100 any
!
```

The following example displays all standard IPv6 ACLs in the running-config of the local switch:

```
switch# show running-config ipv6 access-list standard
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any
!
ipv6 access-list standard ipv6_acl_std_1
 seq 10 deny 2001:2001::/64 count log
```

Related Commands

access-group, access-list, show access-list, show statistics access-list

show running-config ag

Displays the configured N_Port to VF_Port mappings, port grouping information, and other parameters for Access Gateway (AG) mode.

Syntax

show running-config ag *rbridge-id*

Command Default

Displays the AG configuration on local switch when the RBridge ID is not specified.

Parameters

rbridge-id
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display parameters configured for AG mode. This shows the factory-default configuration, unless parameters have been modified by the user.

Consider the following when using LB mode with **show running-config ag** and **show ag** commands:

- The only Port Grouping mode that you can enable or disable is lb mode.
- When lb mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the configured VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When lb mode is enabled in a port group, **show ag** and **show ag map** commands display the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples

The following example displays the running AG configuration for RBridge ID 1.

```
sw0# show running-config rbridge-id 1 ag
  nport 1/0/1
   map fport interface Fcoe 1/1/1 1/1/9 1/1/17 1/1/25 1/1/33 1/1/41 1/1/49 1/1/57
  !
  nport 1/0/2
   map fport interface Fcoe 1/1/2 1/1/10 1/1/18 1/1/26 1/1/34 1/1/42 1/1/50 1/1/58
  !
  nport 1/0/3
   map fport interface Fcoe 1/1/3 1/1/11 1/1/19 1/1/27 1/1/35 1/1/43 1/1/51 1/1/59
  !
  nport 1/0/4
   map fport interface Fcoe 1/1/4 1/1/12 1/1/20 1/1/28 1/1/36 1/1/44 1/1/52 1/1/60
  !
  nport 1/0/5
   map fport interface Fcoe 1/1/5 1/1/13 1/1/21 1/1/29 1/1/37 1/1/45 1/1/53 1/1/61
  !
  nport 1/0/6
   map fport interface Fcoe 1/1/6 1/1/14 1/1/22 1/1/30 1/1/38 1/1/46 1/1/54 1/1/62
  !
  nport 1/0/7
   map fport interface Fcoe 1/1/7 1/1/15 1/1/23 1/1/31 1/1/39 1/1/47 1/1/55 1/1/63
  !
  nport 1/0/8
   map fport interface Fcoe 1/1/8 1/1/16 1/1/24 1/1/32 1/1/40 1/1/48 1/1/56 1/1/64
  !
  pg 0
   nport interface FibreChannel 1/0/1 1/0/2 1/0/3 1/0/4 1/0/5 1/0/6 1/0/7 1/0/8
   modes lb
   rename pg0
  !
timeout fnm 120
counter reliability 25
!
!

sw0# show running-config ag
ag
mapset nport 1/0/1 fports 1/1/1 1/1/92 1/1/173
mapset nport 1/0/2 fports 1/1/24 1/1/105 1/1/186
mapset nport 1/0/3 fports 1/1/37 1/1/118 1/1/199
mapset nport 1/0/4 fports 1/1/410 1/1/1211 1/1/2012
mapset nport 1/0/5 fports 1/1/513 1/1/1314 1/1/2115
mapset nport 1/0/6 fports 1/1/616 1/1/1417 1/1/2218
mapset nport 1/0/7 fports 1/1/719 1/1/1520 1/1/2321
mapset nport 1/0/8 fports 1/1/822 1/1/1623 1/1/24
staticmapadd nport 1/0/1 staticfports
 staticmapadd nport 1/0/2 staticfports
 staticmapadd nport 1/0/3 staticfports
.......
failback 1/0/5 true
failback 1/0/6 true
failback 1/0/7 true
vcs:
fabric-map default
  vlan 1002
  priority 3
  virtual-fabric 128
  fcmap 0E:FC:00
```

Related Commands

show ag, show ag map

show running-config banner

Displays the switch banner.

Syntax

show running-config banner

Modes

Privileged EXEC mode

Examples

To display the switch banner:

```
switch# show running-config banner

banner login "Please don’t disturb the setup on this switch."
```

Related Commands

banner login

show running-config cee-map

Displays the Converged Enhanced Ethernet (CEE) map.

Syntax

show running-config cee-map [**precedence** | **priority-group-table** [*pgid*] | **priority-table** | **remap** { **fabric-priority** | **lossless-priority** }]

Parameters

precedence
Displays only the precedence of the default CEE map.

priority-group-table
Without a specified priority group ID, displays the priority group table for each priority group ID.

pgid
Specifies one priority group ID.

priority-table
Displays the configured priority table map.

remap fabric-priority
Displays the fabric priority for the Brocade VCS Fabric QoS.

remap lossless-priority
Displays the lossless priority for the Brocade VCS Fabric QoS.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display properties of the configured CEE map. Without parameters, the command displays the precedence of the default CEE map, priority group table for each priority group ID, the configured priority table map, and the fabric priority and lossless priority for the Brocade VCS Fabric QoS.

Examples

To display the CEE map:

```
switch(config)# show running-config cee-map

cee-map default
precedence 1
 priority-group-table 1 weight 40 pfc on
 priority-group-table 15.0 pfc off
 priority-group-table 15.1 pfc off
 priority-group-table 15.2 pfc off
 priority-group-table 15.3 pfc off
 priority-group-table 15.4 pfc off
 priority-group-table 15.5 pfc off
 priority-group-table 15.6 pfc off
 priority-group-table 15.7 pfc off
 priority-group-table 2 weight 60 pfc off
 priority-table 2 2 2 1 2 2 2 15.0
 remap fabric-priority priority 0
 remap lossless-prioirty priority 0
!
```

Related Commands

priority-group-table, remap fabric-priority, remap lossless-priority

show running-config class-map

Displays configured class-maps.

Syntax

show running-config class-map

Modes

Privileged EXEC mode

Usage Guidelines

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To display configured class maps:.

```
switch# show running-config class-map

class-map default
match any
```

Related Commands

qos cos

show running-config diag post

Displays the defined POST configuration.

Syntax

show running-config diag post

Modes

Privileged EXEC mode

Examples

```
switch# show running-config diag post

diag post rbridge-id 132
 no enable
switch# show running-config diag post

diag post rbridge-id 132
 enable
```

Related Commands

diag post enable

show running-config dot1x

Displays the IEEE 802.1x Port Authentication configuration.

Syntax

show running-config dot1x [**enable** | **test timeout**]

Parameters

enable

Shows the configured state of globally enabled IEEE 8.02.1x port authentication.

test timeout

Shows the configured timeout value in seconds for the IEEE 802.1x readiness check.

Modes

Privileged EXEC mode

Related Commands

dot1x enable, dot1x test timeout

show running-config dpod

Displays Dynamic Ports on Demand (DPOD) license information.

Syntax

show running-config dpod [*rbridge-id/slot/port*]

Command Default

Displays all port reservations on the local switch.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display port reservations for a specified port or for all ports on the local switch.

This command has no effect on Brocade VDX 8770 switches. These switches do not support the Dynamic Ports on Demand feature.

Examples

To display port reservations for all ports on the local switch:

```
switch# show running-config dpod

dpod 10/0/1
  reserve
!
dpod 10/0/2
  reserve
!
dpod 10/0/3
!
dpod 10/0/4
  reserve
!
dpod 10/0/5
!
dpod 10/0/6
  reserve
!
(Output truncated)
```

To display port reservations on a switch that does not support the DPOD feature:

```
switch# show running-config dpod

%No entries found
```

Related Commands

dpod, show dpod

show running-config fabric route mcast

Displays fabric route multicast configuration information.

Syntax

show running-config fabric route mcast { **rbridge-id** *rbridge-id* | **priority** }

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

priority
Displays the priority value.

Modes

Privileged EXEC mode

Usage Guidelines

The configuration currently effective on the switch is referred to as the running configuration. Any configuration change you make while the switch is online is made to the running configuration.

Examples

These examples display fabric route multicast configuration information:

```
switch# show running-config fabric route mcast

fabric route mcast rbridge-id 2
switch# show running-config fabric route mcast rbridge-id 2 priority

fabric route mcast rbridge-id 2
priority 1
```

Related Commands

fabric route mcast, show fabric route multicast

show running-config fcoe

Displays the running configuration for FCoE.

Syntax

show running-config fcoe [**fabric-map default** | **map default**]

Parameters

fabric-map default
Displays the contents of the fabric map.

map default
Displays the list of available maps.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config fcoe fabric-map default

fcoe
  fabric-map default
    vlan-id 1002
    priority 3
    virtual-fabric 128
    fcmap 0E:FC:00
    advertisement interval 8000
    keep-alive timeout
switch# show running-config fcoe map default

fcoe
map default
  fabric-map default
  cee-map default
```

show running-config fcsp auth

Displays the E_Port-to-EX_Port authentication protocol parameters.

Syntax

show running-config [**rbridge-id** { *rbridge-id* | **all** }] **fcsp auth**

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the E_Port-to-EX_Port authentication protocol parameters such as auth-type, group, hash type, and policy state.

The policy status can be one of the following:. ON, OFF, ACTIVE, or PASSIVE. Refer to the **fcsp auth** command for a description of policy states.

Examples

To display both protocol and policy (auth-type = all, group = 2, hash = md5, and switch policy = off)

```
swe52# show running-config rbridge-id 2 fcsp auth
rbridge-id 2
fcspauth auth-type all
fcspauth group 2
fcspauth hash sha1
fcspauth policy switch active
```

Related Commands

fcsp auth, fcsp auth-secret dhchap, show fcsp auth-secret dh-chap

show running-config hardware

Displays configuration information relating to the flexport on a switch.

Syntax

show running-config hardware { **connector-group** | **flexport** }

Parameters

connector-group

Displays the current configuration of the connector group for the flexport.

flexport

Displays the current configuration of the flexport.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The **show running-config hardware connector-group** command displays the following information:

```
switch# show runn hardware connector-group
hardware
 connector-group 1/0/1
  speed LowMixed
 !
 connector-group 1/0/3
  speed LowMixed
 !
 connector-group 1/0/5
  speed LowMixed
 !
 connector-group 1/0/6
  speed LowMixed
 !
 connector-group 2/0/1
  speed LowMixed
 !
 connector-group 2/0/3
  speed LowMixed
 !
 connector-group 2/0/5
  speed LowMixed
 !
 connector-group 2/0/6
  speed LowMixed
 !
```

History

Release version	Command history
5.0.0	This command was introduced.

show running-config hardware connector

Displays the SFP configurations in the running-config.

Syntax

show running-config hardware connector

Command Default

Displays information for the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To display the SFP configuration on the local switch:

```
switch# show running-config hardware connector
hardware
 connector 0/1
  no sfp breakout
 !
 connector 0/2
  sfp breakout
```

Related Commands

clear support, copy support, show support, sfp breakout

show running-config interface fcoe

Displays the status of FCoE interfaces.

Syntax

show running-config interface fcoe [*vn-number/rbridge-id/front-port-number*]

Parameters

vn-number/rbridge-id/front-port-number
Specifies a valid FCoE port interface.

vn-number
Specifies the VN number for FCoE.

rbridge-id
Specifies an RBridge ID.

front-port-number
Specifies the front port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fcoe

interface Fcoe 1/22/1
 no shutdown
!
interface Fcoe 1/22/2
 no shutdown
!
interface Fcoe 1/22/3
 no shutdown
!
interface Fcoe 1/22/4
 no shutdown
!
interface Fcoe 1/22/5
 no shutdown
!
interface Fcoe 1/22/6
 no shutdown
!
```

show running-config interface FibreChannel

Displays Fibre Channel port attributes.

Syntax

show running-config interface FibreChannel [*rbridge-id/slot/port* [**desire-distance** | **fill-word** | **isl-r_rdy** | **long-distance** | **shutdown** | **speed** | **trunk-enable** | **vc-link-init**]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

desire-distance
Displays the setting of the desired distance attribute.

fill-word
Displays the configured link initialization and fill word primitives for 8 Gbps Fibre Channel ports: idle-idle, arbff-arbff, idle-arbff, or aa-then-ia.

isl-r_rdy
Displays whether R_RDY buffer-to-buffer flow control is enabled for the ISL. VC_RDY flow control is enabled if R_RDY flow control is disabled.

long-distance
Displays the configured long distance mode:

l0—Long distance mode is not configured.

le—Link is up to 10 km.

ld—Distance is determined dynamically.

ls—Distance is determined statically by the user (**desire-distance** command).

shutdown
Displays whether the port is enabled (**no shutdown**) or disabled (**shutdown**).

speed
Displays the configured port speed: auto, 1 Gbps, 2 Gbps, 4 Gbps, or 8 Gbps.

trunk-enable
Displays whether trunking is enabled on the port.

vc-link-init

Displays the configured long distance fill word: idle or arb.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display port attributes for a specified Fibre Channel port or for all Fibre Channel ports on the cluster.

Enter the command without specifying *rbridge-id/slot/port* to obtain a listing of attributes for all Fibre Channel ports. Enter the command with the *rbridge-id/slot/port* parameters to obtain attributes information for a specific port. The values for desire-distance, isl-r_rdy, trunk-enable, and shutdown are always displayed. The values for fill-word, long-distance, speed, and vc-link-init are displayed only if they have been changed from their default values.

Include the attribute name to obtain the setting of that specific attribute only.

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6740), in Brocade VCS Fabric mode, and with the FCoE license installed.

Enter **interface FibreChannel** to set the values.

Examples

To display Fibre Channel port attributes for all ports on a Brocade VDX 6740 switch:

```
switch# show running-config interface FibreChannel

interface FibreChannel 3/0/1
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
interface FibreChannel 3/0/2
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
interface FibreChannel 3/0/3
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 no shutdown
!
(Output truncated)
```

To display Fibre Channel port attributes for one port of a Brocade VDX 6740 switch:

```
switch# show running-config interface FibreChannel 8/0/1

interface FibreChannel 8/0/1
 speed 8gbps
 long-distance ld
 vc-link-init arb
 desire-distance 0
 no isl-r_rdy
 trunk-enable
 shutdown
!
```

To display the setting of a specific attribute on a specific port:

```
switch# show running-config interface FibreChannel 66/0/1 speed

interface FibreChannel 66/0/1
 speed auto
!
```

Related Commands

fill-word, interface, isl-r_rdy, shutdown, speed (Fibre Channel), trunk-enable, vc-link-init

show running-config interface fortygigabitethernet

Displays the status of 40-gigabit Ethernet interfaces.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*]

Command Default

Displays the configuration of all 40-gigabit Ethernet interfaces on the local switch.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display configuration information about all 40-gigabit Ethernet interfaces on a Brocade VDX switch:

```
switch# show running-config interface fortygigabitethernet

interface Forty Gigabit Ethernet 22/0/49
fabric isl enable
fabric trunk enable
no shutdown
!
interface Forty Gigabit Ethernet 22/0/50
fabric isl enable
fabric trunk enable
no shutdown
!
interface Forty Gigabit Ethernet 22/0/51
fabric isl enable
fabric trunk enable
no shutdown
!
interface Forty Gigabit Ethernet 22/0/52
fabric isl enable
fabric trunk enable
sflow enable
no shutdown
!
interface Forty Gigabit Ethernet 22/0/53
fabric isl enable
fabric trunk enable
sflow enable
shutdown
!
interface Forty Gigabit Ethernet 22/0/54
fabric isl enable
fabric trunk enable
```

Related Commands

interface

show running-config interface fortygigabitethernet bpdu-drop

Displays the BPDU drop status of a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **bpdu-drop** [**enable**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Modes

Privileged EXEC mode

Usage Guidelines

STP, RSTP, or MSTP must be configured.

Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples

To display BPDU drop status information for a specific 40-gigabit Ethernet port:

```
switch# show running-config interface fortygigabitethernet 1/0/49 bpdu-drop
```

Related Commands

interface

show running-config interface fortygigabitethernet cee

Displays whether the default CEE map has been applied to a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **cee**

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command does not apply to ISL ports.

Related Commands

cee

show running-config interface fortygigabitethernet channel-group

Displays channel group configuration information for a 40-gigabit Ethernet interface participating in link aggregation.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **channel-group** [**mode** | **type**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

mode
: Displays the mode of link aggregation (active, passive, or on).

type
: Displays the type of link aggregation (802.3ad standards-based LAG, or Brocade proprietary hardware-based trunking).

Modes

Privileged EXEC mode

Usage Guidelines

This command is relevant only to interfaces configured as part of a LAG.

Related Commands

channel-group

show running-config interface fortygigabitethernet description

Displays the description string associated with a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **description**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/52 description

interface fortygigabitethernet 1/0/52
 description Connects to storage device 1
```

Related Commands

description (interfaces), interface

show running-config interface fortygigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **dot1x** [**authentication** | **port-control** | **protocol-version** | **quiet-period** | **reauthMax** | **reauthentication** | **timeout** [**re-authperiod** | **server-timeout** | **supp-timeout** | **tx-period**]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

authentication
Indicates whether 802.1x port-based access control is enabled on the interface.

port-control
Displays the status of port authorization: auto (authentication on the port is enabled), forced authorize, or force unauthorize.

protocol-version
Displays the version number of the dot1x protocol.

quiet-period
Displays the number of seconds between a failed authentication and the next authentication retry.

reauthMax
Displays the maximum number of reauthentication attempts before the port goes into the reauthorized state.

reauthentication
Indicates whether reauthentication is enabled on a port.

timeout
Displays 802.1x timeout values.

re-authperiod
Displays the reauthentication interval in seconds.

server-timeout
Displays the number of seconds the switch waits for a response from the authentication server.

supp-timeout
Displays the number of seconds that the switch waits for a response to the Extensible Authentication Protocol (EAP) frame.

tx-period

Displays the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before retransmitting the request

Modes

Privileged EXEC mode

Examples

To display the 802.1x port-based authentication configuration for a 40-gigabit Ethernet interface:

```
switch# show running-config interface fortygigabitethernet 1/0/49 dot1x

interface fortygigabitethernet 1/0/49
dot1x authentication
dot1x port-control auto
dot1x quiet-period 120
dot1x reauthMax 5
dot1x reauthentication
dot1x timeout server-timeout 60
```

Related Commands

dot1x authentication, dot1x port-control, dot1x quiet-period, dot1x reauthentication, dot1x reauthMax, dot1x timeout re-authperiod, dot1x timeout server-timeout, dot1x timeout supp-timeout, dot1x timeout tx-period

show running-config interface fortygigabitethernet fabric

Displays fabric protocol configuration parameters for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **fabric** [**isl** [**enable**] | **trunk** [**enable**]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

isl [**enable**]
Indicates only the administration and operational state the Inter-Switch Link (ISL).

trunk [**enable**]
Indicates only whether trunking is enabled on the port.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 fabric

interface fortygigabitethernet 1/0/49
 fabric isl enable
 fabric trunk enable
```

Related Commands

fabric isl enable, fabric trunk enable

show running-config interface fortygigabitethernet fcoeport

Displays whether a 40-gigabit Ethernet interface is configured as an FCoE port.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **fcoeport**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Related Commands

fcoe, fcoeport

show running-config interface fortygigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **lacp** [**timeout**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

timeout
: Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Modes

Privileged EXEC mode

Related Commands

lacp timeout

show running-config interface fortygigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **lldp** [**dcbx-version** | **disable** | **iscsi-priority** | **profile**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

dcbx-version
Displays the configured version of the Data Center Bridging Exchange (DCBX) protocol.

disable
Indicates whether LLDP is disabled on the interface.

iscsi-priority
Displays the configured priority that will be advertized in the DCBX iSCSI TLV.

profile
Displays the LLDP profile configured on the interface.

Modes

Privileged EXEC mode

Related Commands

lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile

show running-config interface fortygigabitethernet mac

Displays configured MAC parameters for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **mac** [**access-group**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

access-group
Displays MAC ACLs configured for the specified interface.

Modes

Privileged EXEC mode

Related Commands

mac access-group

show running-config interface fortygigabitethernet mtu

Displays the configured MTU for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **mtu**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 mtu

interface fortygigabitethernet 1/0/49
 mtu 2500
```

Related Commands

ip mtu

show running-config interface fortygigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **port-profile-port**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/50 port-profile-port

interface fortygigabitethernet 1/0/50
port-profile-port
```

Related Commands

port-profile-port

show running-config interface fortygigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **priority-tag**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/51 priority-tag

interface fortygigabitethernet 1/0/51
 priority-tag
```

Related Commands

priority-tag

show running-config interface fortygigabitethernet qos

Displays the Quality of Service (QoS) configuration for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **qos** [**cos** | **cos-mutation** | **cos-traffic-class** | **flowcontrol** [**rx** | **tx**] | **trust** [**cos**]]

Command Default

Displays the full QoS configuration for the interface.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

cos
Displays only the Class of Service (CoS) value configured for the interface.

cos-mutation
Displays the Cos-to-CoS mutation QoS map configured for the interface.

cos-traffic-class
Displays the CoS-to-Traffic Class QoS Map configured for the interface.

flowcontrol
Displays the activation status of QoS flow control on the interface.

rx
Displays the activation status of the receive portion of flow control for the interface.

tx
Displays the activation status of the transmit portion of flow control for the interface.

trust cos
Displays the configured QoS trust mode for the interface.

Modes

Privileged EXEC mode

Related Commands

qos cos, qos cos-mutation, qos cos-traffic-class, qos flowcontrol, qos trust cos, show qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interfaceshow qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interface

show running-config interface fortygigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **rmon** [**collection** [**history** *index* | **stats** *index*]]

Command Default

Displays all RMON collection configuration information.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

collection
Displays configuration information for RMON collections.

history
Displays configuration information for RMON history collections.

index
Specifies a valid RMON history collection index value.

stats
Displays configuration information for RMON statistics collections.

index
Specifies a valid RMON collection control index value.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 rmon collection

interface fortygigabitethernet 1/0/49
 rmon collection stats 10 owner RMON_SNMP
 rmon collection history 10 owner RMON_SNMP
```

Related Commands

rmon collection history, rmon collection stats

show running-config interface fortygigabitethernet sflow

Displays the sFlow configuration for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **sflow** [**enable** | **polling-interval** | **sample-rate**]

Command Default

Displays all sFlow configuration information for the port.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Displays whether sFlow is enabled for the port.

polling-interval
: Displays the configured maximum number of seconds between successive samples of counters to be sent to the collector.

sample-rate
: Displays the number of packets that are skipped before the next sample is taken for the interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/53 sflow

interface fortygigabitethernet 1/0/53
 sflow enable
 sflow polling-interval 10
 sflow sample-rate 100
```

Related Commands

sflow enable (interface version), sflow polling-interval (interface version), sflow sample-rate (interface version)

show running-config interface fortygigabitethernet shutdown

Displays whether a 40-gigabit Ethernet interface is enabled.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **shutdown**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/52 shutdown

interface fortygigabitethernet 1/0/52
 no shutdown
```

Related Commands

shutdown

show running-config interface fortygigabitethernet switchport

Displays the configured switching characteristics for the 40-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id* | *slot* | *port*] **switchport** [**access** [**vlan**] | **mode** | **trunk** [**allowed** [**vlan**] | **native-vlan** | **tag** [**native-vlan**]]

Command Default

Displays all configured Layer 2 switching characteristics for the port.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

access
Displays whether the Layer 2 interface is configured as access.

access vlan
Displays whether the specific VLAN on the Layer 2 interface is configured as access.

mode
Displays whether the Layer 2 interface is configured for access, trunk or converged.

trunk
Displays whether the Layer 2 interface is configured for trunk.

trunk allowed
Displays the configuration settings that determine the VLANs that will transmit and receive through the Layer 2 interface.

trunk allowed vlan
Displays the configuration settings for a specific VLAN.

trunk allowed native-vlan
Displays the configured native VLAN characteristics of the Layer 2 trunk interface for classifying untagged traffic.

trunk tag
Displays whether tagging is enabled.

tag native-vlan
Displays native VLAN tags.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 switchport

interface fortygigabitethernet 1/0/49
 switchport
 switchport mode access
 switchport access vlan 1
```

Related Commands

switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan

show running-config interface fortygigabitethernet udld

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 40-gigabit Ethernet interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **udld enable**

Command Default

This command has no defaults.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Indicates whether UDLD is enabled on the interface.

Modes

Privileged EXEC mode

show running-config interface fortygigabitethernet vlan

Displays information about VLAN classification groups for a 40-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface fortygigabitethernet [*rbridge-id/slot/port*] **vlan** [**classifier** [**activate** [**group**]]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

classifier
Displays VLAN classifier commands for the Layer 2 interface.

activate
Displays VLAN classifier activate commands for the Layer 2 interface.

group
Displays VLAN classifier activate group commands for the Layer 2 interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 vlan

interface fortygigabitethernet 1/0/49
vlan classifier activate group 1 vlan 2
```

Related Commands

show vlan classifier, switchport, vlan classifier activate group, vlan classifier group, vlan classifier rule

show running-config interface gigabitethernet

Displays the status of 1-gigabit Ethernet interfaces.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*]

Command Default

Displays the configuration of all 1-gigabit Ethernet interfaces on the local switch.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display configuration information about all 1-gigabit Ethernet interfaces on the local switch:

```
switch# show running-config interface gigabitethernet

interface Gigabit Ethernet 22/0/1
 description tests
 channel-group 2 mode active type standard
 lacp timeout long
 sflow enable
 no shutdown
!
interface Gigabit Ethernet 22/0/2
 channel-group 2 mode active type standard
 lacp timeout long
 no shutdown
!
interface Gigabit Ethernet 22/0/3
 channel-group 2 mode active type standard
 lacp timeout long
 no shutdown
!
interface Gigabit Ethernet 22/0/4
 no shutdown
!
interface Gigabit Ethernet 22/0/5
 no shutdown
!
interface Gigabit Ethernet 22/0/6
 no shutdown
!
interface Gigabit Ethernet 22/0/7
 no shutdown
(Output truncated)
```

Related Commands

interface

show running-config interface gigabitethernet bpdu-drop

Displays the BPDU drop status of a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **bpdu-drop** [**enable**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Modes

Privileged EXEC mode

Usage Guidelines

STP, RSTP, or MSTP must be configured.

Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples

To display BPDU drop status information for a specific 1-gigabit Ethernet port:

```
switch# show running-config interface gigabitethernet 1/0/7 bpdu-drop
```

Related Commands

interface

show running-config interface gigabitethernet channel-group

Displays channel group configuration information for an interface participating in link aggregation.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **channel-group** [**mode** | **type**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

mode
: Displays the mode of link aggregation (active, passive, or on).

type
: Displays the type of link aggregation (802.3ad standards-based LAG, or Brocade proprietary hardware-based trunking).

Modes

Privileged EXEC mode

Usage Guidelines

This command is relevant only to interfaces configured as part of a LAG.

Related Commands

channel-group

show running-config interface gigabitethernet description

Displays the description string associated with a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **description**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/7 description

interface Gigabit Ethernet 1/0/7
description Connects to storage device 1
```

Related Commands

description (interfaces), interface

show running-config interface gigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **dot1x** [**authentication** | **port-control** | **protocol-version** | **quiet-period** | **reauthMax** | **reauthentication** | **timeout** [**re-authperiod** | **server-timeout** | **supp-timeout** | **tx-period**]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

authentication
Indicates whether 802.1x port-based access control is enabled on the interface.

port-control
Displays the status of port authorization: auto (authentication on the port is enabled), forced authorize, or force unauthorize.

protocol-version
Displays the version number of the dot1x protocol.

quiet-period
Displays the number of seconds between a failed authentication and the next authentication retry.

reauthMax
Displays the maximum number of reauthentication attempts before the port goes into the reauthorized state.

reauthentication
Indicates whether reauthentication is enabled on a port.

timeout
Displays 802.1x timeout values.

re-authperiod
Displays the reauthentication interval in seconds.

server-timeout
Displays the number of seconds the switch waits for a response from the authentication server.

supp-timeout
Displays the number of seconds that the switch waits for a response to the Extensible Authentication Protocol (EAP) frame.

tx-period
Displays the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before retransmitting the request

Modes

Privileged EXEC mode

Examples

To display the 802.1x port-based authentication configuration for a 1-gigabit Ethernet interface:

```
switch# show running-config interface gigabitethernet 1/0/7 dot1x

interface Gigabit Ethernet 1/0/7
 dot1x authentication
 dot1x port-control auto
 dot1x quiet-period 120
 dot1x reauthMax 5
 dot1x reauthentication
 dot1x timeout server-timeout 60
```

Related Commands

dot1x authentication, dot1x port-control, dot1x quiet-period, dot1x reauthentication, dot1x reauthMax, dot1x timeout re-authperiod, dot1x timeout server-timeout, dot1x timeout supp-timeout, dot1x timeout tx-period

show running-config interface gigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **lacp** [**timeout**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

timeout
: Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Modes

Privileged EXEC mode

Related Commands

lacp timeout

show running-config interface gigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **lldp** [**dcbx-version** | **disable** | **iscsi-priority** | **profile**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

dcbx-version
Displays the configured version of the Data Center Bridging Exchange (DCBX) protocol.

disable
Indicates whether LLDP is disabled on the interface.

iscsi-priority
Displays the configured priority that will be advertized in the DCBX iSCSI TLV.

profile
Displays the LLDP profile configured on the interface.

Modes

Privileged EXEC mode

Related Commands

lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile

show running-config interface gigabitethernet mac

Displays configured MAC parameters for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **mac** [**access-group**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

access-group
Displays MAC ACLs configured for the specified interface.

Modes

Privileged EXEC mode

Related Commands

mac access-group

show running-config interface gigabitethernet mtu

Displays the configured MTU for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **mtu**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 mtu

interface Gigabit Ethernet 1/0/8
 mtu 2500
!
```

Related Commands

ip mtu

show running-config interface gigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **port-profile-port**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 port-profile-port

interface Gigabit Ethernet 1/0/8
 port-profile-port
```

Related Commands

port-profile-port

show running-config interface gigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **priority-tag**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 priority-tag

interface Gigabit Ethernet 1/0/8
 priority-tag
```

Related Commands

priority-tag

show running-config interface gigabitethernet qos

Displays the Quality of Service (QoS) configuration for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **qos** [**cos** | **cos-mutation** | **cos-traffic-class** | **flowcontrol** [**rx** | **tx**] | **trust** [**cos**]]

Command Default

Displays the full QoS configuration for the interface.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

cos
: Displays only the Class of Service (CoS) value configured for the interface.

cos-mutation
: Displays the Cos-to-CoS mutation QoS map configured for the interface.

cos-traffic-class
: Displays the CoS-to-Traffic Class QoS Map configured for the interface.

flowcontrol
: Displays the activation status of QoS flow control on the interface.

rx
: Displays the activation status of the receive portion of flow control for the interface.

tx
: Displays the activation status of the transmit portion of flow control for the interface.

trust cos
: Displays the configured QoS trust mode for the interface.

Modes

Privileged EXEC mode

Related Commands

qos cos, qos cos-mutation, qos cos-traffic-class, qos flowcontrol, qos trust cos, show qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interface

show running-config interface gigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **rmon** [**collection** [**history** *index* | **stats** *index*]]

Command Default

Displays all RMON collection configuration information.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

collection
: Displays configuration information for RMON collections.

history
: Displays configuration information for RMON history collections.

stats
: Displays configuration information for RMON statistics collections.

index
: Specifies a valid RMON collection control index value.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 rmon collection

interface Gigabit Ethernet 1/0/8
 rmon collection stats 10 owner RMON_SNMP
 rmon collection history 10 owner RMON_SNMP
```

Related Commands

rmon collection history, rmon collection stats

show running-config interface gigabitethernet sflow

Displays the sFlow configuration for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **sflow** [**enable** | **polling-interval** | **sample-rate**]

Command Default

Displays all sFlow configuration information for the port.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

enable
Displays whether sFlow is enabled for the port.

polling-interval
Displays the configured maximum number of seconds between successive samples of counters to be sent to the collector.

sample-rate
Displays the number of packets that are skipped before the next sample is taken for the interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 sflow

interface Gigabit Ethernet 1/0/8
 sflow enable
 sflow polling-interval 10
 sflow sample-rate 100
!
```

Related Commands

sflow enable (interface version), sflow polling-interval (interface version), sflow sample-rate (interface version)

show running-config interface gigabitethernet shutdown

Displays whether a 1-gigabit Ethernet interface is enabled.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **shutdown**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 shutdown

interface Gigabit Ethernet 1/0/8
 no shutdown
```

Related Commands

shutdown

show running-config interface gigabitethernet switchport

Displays the configured switching characteristics for the 1-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **switchport** [**access** [**vlan**] | **mode** | **trunk** [**allowed** [**vlan**] | **native-vlan** | **tag** [**native-vlan**]]

Command Default

Displays all configured Layer 2 switching characteristics for the port.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

access
Displays whether the Layer 2 interface is configured as access.

access vlan
Displays whether the specific VLAN on the Layer 2 interface is configured as access.

mode
Displays whether the Layer 2 interface is configured for access, trunk or converged.

trunk
Displays whether the Layer 2 interface is configured for trunk.

trunk allowed
Displays the configuration settings that determine the VLANs that will transmit and receive through the Layer 2 interface.

trunk allowed vlan
Displays the configuration settings for a specific VLAN.

trunk allowed native-vlan
Displays the configured native VLAN characteristics of the Layer 2 trunk interface for classifying untagged traffic.

trunk tag
Displays whether tagging is enabled.

tag native-vlan
Displays tags for the native VLAN.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 switchport

interface Gigabit Ethernet 1/0/8
 switchport
 switchport mode access
 switchport access vlan 1
```

Related Commands

switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan

show running-config interface gigabitethernet udld

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 1-gigabit Ethernet interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **udld enable**

Command Default

This command has no defaults.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Indicates whether UDLD is enabled on the interface.

Modes

Privileged EXEC mode

show running-config interface gigabitethernet vlan

Displays information about VLAN classification groups for the 1-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface gigabitethernet [*rbridge-id/slot/port*] **vlan** [**classifier** [**activate** [**group**]]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

classifier
Displays VLAN classifier commands for the Layer 2 interface.

activate
Displays VLAN classifier activate commands for the Layer 2 interface.

group
Displays VLAN classifier activate group commands for the Layer 2 interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface gigabitethernet 1/0/8 vlan

interface Gigabit Ethernet 1/0/8
vlan classifier activate group 1 vlan 2
```

Related Commands

show vlan classifier, switchport, vlan classifier activate group, vlan classifier group, vlan classifier rule

show running-config interface management

Displays the management interface configuration.

Syntax

show running-config interface management [*rbridge-id/* | *port*] [*ip*] **access group**

Parameters

rbridge-id/ | *port*

Specifies the management interface to be displayed as the RBridge ID followed by a slash (/) and the port number.

On standalone platforms, the port number for the management port is always 0.On a modular switches with two redundant management modules, can configure two management ports: 1 and 2.

ip

Displays the IP addresses configured for the management interface.Use **access-group** to display selected addresses only.

access-group

Displays the access lists (ACLs) configured on the management interface.

Modes

Privileged EXEC mode

Examples

This example displays the authentication mode:

```
switch# show running-config interface Management 2/2

interface Management 2/2
  .
  ip access-group extdACL5
```

Related Commands

interface management, ip access-list, show running-config ip access-list

show running-config interface port-channel

Displays the status of port-channel interfaces.

Syntax

show running-config interface port-channel [*number*]

Command Default

Displays the configuration of all port channel interfaces on the local switch.

Parameters

number

Specifies a valid port-channel number.

Modes

Privileged EXEC mode

Examples

To display configuration information about all port channel interfaces on a Brocade switch:

```
switch# show running-config interface port-channel

interface port-channel 1
description 1
shutdown
!
interface port-channel 2
switchport
switchport mode access
switchport access vlan 1
shutdown
!
interface port-channel 3
shutdown
```

Related Commands

interface

show running-config interface tengigabitethernet

Displays the status of 10-gigabit Ethernet interfaces.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*]

Command Default

Displays the configuration of all 10-gigabitEthernet interfaces on the local switch.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display configuration information about all 10-gigabit Ethernet interfaces on a Brocade VDX switch:

```
switch# show running-config interface tengigabitethernet

interface Ten Gigabit Ethernet 22/0/49
fabric isl enable
fabric trunk enable
no shutdown
!
interface Ten Gigabit Ethernet 22/0/50
fabric isl enable
fabric trunk enable
no shutdown
!
interface Ten Gigabit Ethernet 22/0/51
fabric isl enable
fabric trunk enable
no shutdown
!
interface Ten Gigabit Ethernet 22/0/52
fabric isl enable
fabric trunk enable
sflow enable
no shutdown
!
interface Ten Gigabit Ethernet 22/0/53
fabric isl enable
fabric trunk enable
sflow enable
shutdown
!
interface Ten Gigabit Ethernet 22/0/54
fabric isl enable
fabric trunk enable
```

Related Commands

interface

show running-config interface tengigabitethernet bpdu-drop

Displays the BPDU drop status of a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **bpdu-drop** [**enable**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Modes

Privileged EXEC mode

Usage Guidelines

STP, RSTP, or MSTP must be configured.

Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples

To display BPDU drop status information for a specific 10-gigabit Ethernet port:

```
switch# show running-config interface tengigabitethernet 1/0/49 bpdu-drop
```

Related Commands

interface

show running-config interface tengigabitethernet cee

Displays whether the default CEE map has been applied to a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **cee**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command does not apply to ISL ports.

Related Commands

cee

show running-config interface tengigabitethernet channel-group

Displays channel group configuration information for a 10-gigabit Ethernet interface participating in link aggregation.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **channel-group** [**mode** | **type**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

mode
: Displays the mode of link aggregation (active, passive, or on).

type
: Displays the type of link aggregation (802.3ad standards-based LAG, or Brocade proprietary hardware-based trunking).

Modes

Privileged EXEC mode

Usage Guidelines

This command is relevant only to interfaces configured as part of a LAG.

Related Commands

channel-group

show running-config interface tengigabitethernet description

Displays the description string associated with a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **description**

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/52 description

interface tengigabitethernet 1/0/52
 description Connects to storage device 1
```

Related Commands

description (interfaces), interface

show running-config interface tengigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **dot1x** [**authentication** | **port-control** | **protocol-version** | **quiet-period** | **reauthMax** | **reauthentication** | **timeout** [**re-authperiod** | **server-timeout** | **supp-timeout** | **tx-period**]]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

authentication
: Indicates whether 802.1x port-based access control is enabled on the interface.

port-control
: Displays the status of port authorization: auto (authentication on the port is enabled), forced authorize, or force unauthorize.

protocol-version
: Displays the version number of the dot1x protocol.

quiet-period
: Displays the number of seconds between a failed authentication and the next authentication retry.

reauthMax
: Displays the maximum number of reauthentication attempts before the port goes into the reauthorized state.

reauthentication
: Indicates whether reauthentication is enabled on a port.

timeout
: Displays 802.1x timeout values.

re-authperiod
: Displays the reauthentication interval in seconds.

server-timeout
: Displays the number of seconds the switch waits for a response from the authentication server.

supp-timeout
: Displays the number of seconds that the switch waits for a response to the Extensible Authentication Protocol (EAP) frame.

tx-period

Displays the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before retransmitting the request

Modes

Privileged EXEC mode

Examples

To display the 802.1x port-based authentication configuration for a 10-gigabit Ethernet interface:

```
switch# show running-config interface tengigabitethernet 1/0/49 dot1x

interface tengigabitethernet 1/0/49
dot1x authentication
dot1x port-control auto
dot1x quiet-period 120
dot1x reauthMax 5
dot1x reauthentication
dot1x timeout server-timeout 60
```

Related Commands

dot1x authentication, dot1x port-control, dot1x quiet-period, dot1x reauthentication, dot1x reauthMax, dot1x timeout re-authperiod, dot1x timeout server-timeout, dot1x timeout supp-timeout, dot1x timeout tx-period

show running-config interface tengigabitethernet fabric

Displays fabric protocol configuration parameters for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **fabric** [**isl** [**enable**] | **trunk** [**enable**]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

isl [**enable**]
Indicates only the administration and operational state of the Inter-Switch Link (ISL).

trunk [**enable**]
Indicates only whether trunking is enabled on the port.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display ISL and trunking status for the specified 10-gigabit Ethernet interface.

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 fabric

interface tengigabitethernet 1/0/49
 fabric isl enable
 fabric trunk enable
```

Related Commands

fabric isl enable, fabric trunk enable

show running-config interface tengigabitethernet fcoeport

Displays whether a 10-gigabit Ethernet interface is configured as an FCoE port.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **fcoeport**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Related Commands

fcoe, fcoeport

show running-config interface tengigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **lacp** [**timeout**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

timeout
: Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Modes

Privileged EXEC mode

Related Commands

lacp timeout

show running-config interface tengigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **lldp** [**dcbx-version** | **disable** | **iscsi-priority** | **profile**]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

dcbx-version
Displays the configured version of the Data Center Bridging Exchange (DCBX) protocol.

disable
Indicates whether LLDP is disabled on the interface.

iscsi-priority
Displays the configured priority that will be advertized in the DCBX iSCSI TLV.

profile
Displays the LLDP profile configured on the interface.

Modes

Privileged EXEC mode

Related Commands

lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile

show running-config interface tengigabitethernet mac

Displays configured MAC parameters for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **mac** [**access-group**]

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

access-group
: Displays MAC ACLs configured for the specified interface.

Modes

Privileged EXEC mode

Related Commands

mac access-group

show running-config interface tengigabitethernet mtu

Displays the configured MTU for a 10 gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **mtu**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 mtu

interface tengigabitethernet 1/0/49
 mtu 2500
```

Related Commands

ip mtu

show running-config interface tengigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **port-profile-port**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/50 port-profile-port

interface tengigabitethernet 1/0/50
port-profile-port
```

Related Commands

port-profile-port

show running-config interface tengigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **priority-tag**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/51 priority-tag

interface tengigabitethernet 1/0/51
 priority-tag
```

Related Commands

priority-tag

show running-config interface tengigabitethernet qos

Displays the quality of service (QoS) configured for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **qos** [**cos** | **cos-mutation** | **cos-traffic-class** | **flowcontrol** [**rx** | **tx**] | **trust** [**cos**]]

Command Default

Displays the full QoS configuration for the interface.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

cos
: Displays only the Class of Service (CoS) value configured for the interface.

cos-mutation
: Displays the Cos-to-CoS mutation QoS map configured for the interface.

cos-traffic-class
: Displays the CoS-to-Traffic Class QoS Map configured for the interface.

flowcontrol
: Displays the activation status of QoS flow control on the interface.

rx
: Displays the activation status of the receive portion of flow control for the interface.

tx
: Displays the activation status of the transmit portion of flow control for the interface.

trust cos
: Displays the configured QoS trust mode for the interface.

Modes

Privileged EXEC mode

Related Commands

qos cos, qos cos-mutation, qos cos-traffic-class, qos flowcontrol, show qos flowcontrol interface, show qos interface, show qos queue interface, show qos rcv-queue interface

show running-config interface tengigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **rmon** [**collection** [**history** *index* | **stats** *index*]]

Command Default

Displays all RMON collection configuration information.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

collection
Displays configuration information for RMON collections.

history
Displays configuration information for RMON history collections.

index
Specifies a valid RMON history collection index value.

stats
Displays configuration information for RMON statistics collections.

index
Specifies a valid RMON collection control index value.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 rmon collection

interface tengigabitethernet 1/0/49
 rmon collection stats 10 owner RMON_SNMP
 rmon collection history 10 owner RMON_SNMP
```

Related Commands

rmon collection history, rmon collection stats

show running-config interface tengigabitethernet sflow

Displays the sFlow configuration for a 10-gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **sflow** [**enable** | **polling-interval** | **sample-rate**]

Command Default

Displays all sFlow configuration information for the port.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Displays whether sFlow is enabled for the port.

polling-interval
: Displays the configured maximum number of seconds between successive samples of counters to be sent to the collector.

sample-rate
: Displays the number of packets that are skipped before the next sample is taken for the interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/53 sflow

interface tengigabitethernet 1/0/53
 sflow enable
 sflow polling-interval 10
 sflow sample-rate 100
```

Related Commands

sflow enable (interface version), sflow polling-interval (interface version), sflow sample-rate (interface version)

show running-config interface tengigabitethernet shutdown

Displays whether a 10-gigabit Ethernet interface is enabled.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **shutdown**

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/52 shutdown

interface tengigabitethernet 1/0/52
 no shutdown
```

Related Commands

shutdown

show running-config interface tengigabitethernet switchport

Displays the configured switching characteristics for the 10-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id* | *slot* | *port*] **switchport** [**access** [**vlan**] | **mode** | **trunk** [**allowed** [**vlan**] | **native-vlan** | **tag** [**native-vlan**]]

Command Default

Displays all configured Layer 2 switching characteristics for the port.

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

access
Displays whether the Layer 2 interface is configured as access.

access vlan
Displays whether the specific VLAN on the Layer 2 interface is configured as access.

mode
Displays whether the Layer 2 interface is configured for access, trunk or converged.

trunk
Displays whether the Layer 2 interface is configured for trunk.

trunk allowed
Displays the configuration settings that determine the VLANs that will transmit and receive through the Layer 2 interface.

trunk allowed vlan
Displays the configuration settings for a specific VLAN.

trunk allowed native-vlan
Displays the configured native VLAN characteristics of the Layer 2 trunk interface for classifying untagged traffic.

trunk tag
Displays whether tagging is enabled.

tag native-vlan
Displays tags for the native VLAN.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 switchport

interface tengigabitethernet 1/0/49
 switchport
 switchport mode access
 switchport access vlan 1
```

Related Commands

switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan

show running-config interface tengigabitethernet udld

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 10 Gigabit Ethernet interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **udld enable**

Command Default

This command has no defaults.

Parameters

rbridge-id
: Specifies an RBridge ID.

slot
: Specifies a valid slot number.

port
: Specifies a valid port number.

enable
: Indicates whether UDLD is enabled on the interface.

Modes

Privileged EXEC mode

show running-config interface tengigabitethernet vlan

Displays information about VLAN classification groups for a 10-gigabit Ethernet Layer 2 interface.

Syntax

show running-config interface tengigabitethernet [*rbridge-id/slot/port*] **vlan** [**classifier** [**activate** [**group**]]]

Parameters

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

classifier
Displays VLAN classifier commands for the Layer 2 interface.

activate
Displays VLAN classifier activate commands for the Layer 2 interface.

group
Displays VLAN classifier activate group commands for the Layer 2 interface.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 vlan

interface tengigabitethernet 1/0/49
vlan classifier activate group 1 vlan 2
```

Related Commands

show vlan classifier, switchport, vlan classifier activate group, vlan classifier group, vlan classifier rule

show running-config interface vlan

Displays the status of VLAN interfaces.

Syntax

show running-config interface vlan [*vlan_id*] [**arp-ageing-timeout** | **description** | **ip** | **mac access-group** | **shutdown** | **spanning-tree**]

Command Default

Displays the configuration of all VLAN interfaces on the local switch.

Parameters

vlan_id
Specifies a VLAN.

arp-ageing-timeout
Displays the configured interface timeout value in minutes for the Address Resolution Protocol (ARP) for VLANs.

description
Displays the description text entered for each VLAN or for the specified VLAN.

ip
Displays IP configuration information for VLANs.

mac access-group
Displays MAC ACLs configured for VLANs.

shutdown
Specifies whether the VLAN interface is enabled.

spanning-tree
Displays spanning tree configuration information for VLANs.

Modes

Privileged EXEC mode

Related Commands

interface, show running-config interface vlan ip

show running-config interface vlan ip

Displays the IP configuration of VLAN interfaces.

Syntax

show running-config interface vlan [*vlan_id*] **ip** [**address** | **igmp** [**last-member-query-interval** | **query-interval** | **query-max-response-time** | **snooping** [**enable** | **fast-leave** | **mrouter** | **mrouter-timeout** | **querier**] | **static-group** *static-group-address*] | **mtu** | **proxy-arp**]

Command Default

Displays configured information for all VLAN interfaces on the local switch.

Parameters

vlan_id
Specifies a VLAN.

address
Displays the IP address configured for VLANs.

igmp
Displays whether the Internet Group Management Protocol (IGMP) is enabled for VLANs.

last-member-query-interval
Displays the amount of time in seconds that the IGMP router waits to receive a response to a group query message.

query-interval
Displays the amount of time in seconds between IGMP query messages sent by the switch.

query-max-response-time
Displays the configured maximum response time in seconds for IGMP queries.

snooping
Displays IGMP snooping configuration information for VLANs.

enable
Indicates whether IGMP snooping is enabled for specified VLANs.

fast-leave
Indicates if snooping fast leave is enabled.

mrouter
Displays multicast router port information for the VLAN.

mrouter-timeout
Displays the configured multicast router IGMP timeout value in seconds.

querier
Indicates if IGMP snooping querier is configured.

static-group
Displays configured static group membership entries.

static-group-address
Specifies an IPv4 address to return static group information about.

mtu
Displays the MTU configured for each VLAN.

proxy-arp
Indicates whether a proxy ARP is configured for VLAN interfaces.

Modes

Privileged EXEC mode

Examples

To display IP configuration information for all configured VLANs:

```
switch# show running-config interface vlan ip

interface Vlan 1
!
interface Vlan 2
ip igmp query-interval 200
ip igmp query-max-response-time 15
ip igmp snooping enable
```

Related Commands

interface management, ip access-list, show running-config interface management

show running-config ip access-list

Displays a list of IPv4 ACLs defined on the switch, including the rules they contain.

Syntax

show running-config ip access-list [**standard** | **extended**] [*ACL_name*]

Parameters

standard | **extended**
Specifies the ACL type. Not specifying the ACL type displays all IPv4 standard and extended ACLs.

ACL_name
Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

To display details of IPv4 ACLs bound to interfaces, use the **show access-list ip** command.

Examples

The following example displays the IPv4 ACLs configured on the switch.

```
switch# show running-config ip access-list

ip access-list standard stdACL3
  seq 5 permit host 10.20.33.4
  seq 7 permit any
ip access-list extended extdACL5
  seq 5 deny tcp host 10.24.26.145 any eq 23
  seq 7 deny tcp any any eq 80
  seq 10 deny udp any any range 10 25
  seq 15 permit tcp any
ip access-list extended extdACLwithNoRules
```

Related Commands

interface management, ip access-group, ip access-list, show running-config interface management, show access-list, show statistics access-list

show running-config ip dns

Displays the domain name service (DNS) parameters. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers.

Syntax

show running-config ip dns

Modes

Privileged EXEC mode

Examples

To display the configured DNS parameters:

```
switch# show running-config ip dns

ip dns domain-name brocade.com
ip dns name-server 10.70.20.1
ip dns name-server 10.70.20.10
```

Related Commands

ip dns

show running-config ip igmp

Displays IGMP configuration information.

Syntax

show running-config ip igmp [**snooping** [**enable**]]

Parameters

snooping

Displays IGMP snooping configuration information.

enable

Displays whether IGMP snooping is enabled.

Modes

Privileged EXEC mode

Examples

To display IGMP configuration information:

```
switch# show running-config ip igmp
```

Related Commands

ip igmp snooping enable, ip igmp snooping enable (global version)

show running-config ip route

Displays routing information.

Syntax

show running-config ip route [**routing-table**]

Parameters

routing-table

Displays a specific route to a specific destination.

Modes

Privileged EXEC mode

show running-config ldap-server

Displays the SSH server status in the running-config.

Syntax

show running-config ldap-server [**host** *ipaddr* | **host-name**]

Parameters

host

Identifies the IPv4 address of the host.

ipaddress

IPv4 address of the host.

host-name

Name of the host.

Modes

Privileged EXEC mode

Usage Guidelines

LDAP server configuration is placed at the beginning of the running-config and is part of the global configuration of the switch. LDAP is enabled by default and no entry is shown in the running-config when set to default.

Attributes with default values will not be displayed.

Examples

```
switch# show running-config ldap-server host 10.24.65.6

ldap-server host 10.24.65.6
 port            3890
 domain              security.brocade.com
 retries             3
!
switch#
```

Related Commands

certutil import ldapca, ldap-server host, ldap-server maprole

show running-config line

Displays command line session configuration information.

Syntax

show running-config line [**vty** [**exec-timeout**]]

Parameters

vty

Displays the terminal type.

exec-timeout

Displays the configured idle time in minutes before the command line session automatically logs off.

Modes

Privileged EXEC mode

Related Commands

interface

show running-config logging

Displays the configuration of the logging facilities on the local switch.

Syntax

show running-config logging

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To display the logging facilities configured on the local switch:

```
switch# show running-config logging

logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
```

Related Commands

show running-config logging auditlog class, show running-config logging syslog-server

show running-config logging auditlog class

Displays the severity level configured for the audit log class.

Syntax

show running-config logging auditlog class

Command Default

Displays the information for the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display audit log classes enabled on the switch:

```
switch# show running-config logging auditlog class

logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
```

Related Commands

clear logging auditlog, clear logging raslog

show running-config logging raslog

Displays the severity level configured for the RASLog console.

Syntax

show running-config logging raslog

Command Default

Displays the RASLog console configuration.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the configured severity levels for the RASlog console. Valid values consist of one of the following: INFO, WARNING, ERROR, or CRITICAL.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display the severity level configured for the RASlog console:

```
switch# show running-config logging raslog

logging raslog console INFO
```

Related Commands

clear logging raslog, logging raslog console, show running-config logging

show running-config logging syslog-facility

Displays the syslog facility log level.

Syntax

show running-config logging syslog-facility [**local**]

Command Default

Displays the local configuration.

Parameters

local

Displays the local syslog facility level.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display the syslog daemon IP addresses configured on a switch:

```
switch# show running-config logging syslog-facility

logging syslog-facility local LOG_LOCAL7
```

Related Commands

logging syslog-server, show running-config logging syslog-server

show running-config logging syslog-server

Displays the syslog server configuration.

Syntax

show running-config logging syslog-server

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the servers that are running the syslogd daemon and to which system messages are sent. Servers are specified in the configuration database by IP address.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display the syslog daemon IP addresses configured on a switch:

```
switch# show running-config logging syslog-server

logging syslog-server 10.17.17.203
 secure port 6514
!
logging syslog-server 10.17.17.204
```

Related Commands

logging syslog-server

show running-config mac-address-table

Displays configuration information about MAC interfaces and configurations.

Syntax

show running-config monitor mac-address-table [**aging-time** | **static**]

Command Default

Default aging time is 300 seconds.

Parameters

aging-time

Specifies the aging time value (in seconds).

static

Specifies a static MAC address.

Modes

Privileged EXEC mode

show running-config monitor

Displays configuration information about the monitor session.

Syntax

show running-config monitor { **session** *session_number* { **description** } }

Parameters

session *session_number*

The session number to display.

description

Displays the session's description.

Modes

Privileged EXEC mode

Examples

To display the monitor information:

```
switch# show running-config monitor

monitor session 22
```

show running-config nas server-ip

Displays information about the specified Auto NAS (automatic network attached storage) interface.

Syntax

show running-config nas server-ip

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Related Commands

backup-advertisement-interval, clear nas statistics, nas auto-qos, nas server-ip, show nas statistics, show system internal nas, show cee maps

show running-config ntp

Displays the Network Time Protocol (NTP) server configuration.

Syntax

show running-config ntp

Modes

Privileged EXEC mode

Examples

To display the configured NTP server

```
switch# show running-config ntp
ntp server 172.26.1.159
```

Related Commands

ntp server, show ntp status

show running-config ntp authentication-key

Displays the currently configured authentication key for accessing the NTP server.

Syntax

show running-config ntp authentication-key

Modes

Privileged EXEC mode

Examples

Typical command output:

```
device# show running-config ntp authentication-key

ntp authentication-key 10 sha1 "cXGFY75bvKpJruCYEiwxjw==\n"encryption-level 7
```

History

Release version	Command history
5.0.2	This command was introduced.

show running-config overlay-gateway

Displays the configured characteristics for an overlay gateway.

Syntax

show running-config overlay-gateway [*gateway_name*]

Parameters

gateway_name

Specifies the overlay-gateway name. Since Network OS supports only one overlay-gateway on a switch, you do not need to enter this parameter. The default name is "gateway1".

Modes

Privileged EXEC mode

Command Output

The **show running-config overlay-gateway** command displays the following information:

Output field	Description
mac access-group	Specifies the name of a Layer 2 access control list (ACL) applied to the overlay gateway.
ip access-group	Specifies the name of an IPv4 ACL applied to the overlay gateway.
ipv6 access-group	Specifies the name of an IPv6 ACL applied to the overlay gateway.

Examples

The following example displays the overlay-gateway running configuration for an overlay gateway that includes multiple sites.

```
sw0# show running-config overlay-gateway
overlay-gateway gw121
type layer2-extension
ip interface Loopback 11
attach rbridge-id add 1-2
map vlan 1 vni 5001
map vlan 10 vni 5010
map vlan 2 vni 5002
map vlan 3 vni 5003
map vlan 4 vni 5004
map vlan 5 vni 5005
map vlan 6 vni 5006
map vlan 7 vni 5007
map vlan 8 vni 5008
map vlan 9 vni 5009
site b
  ip address 2.2.2.2
  extend vlan add 3-4
!
site br
  ip address 3.3.3.3
  extend vlan add 5-6
!
site mu
  ip address 4.4.4.4
  extend vlan add 7-10
!
site san
  ip address 1.1.1.1
  extend vlan add 1-2
!
enable statistics direction both vlan add 5-10
monitor session 11 direction both remote-endpoint any vlan add 5-10
sflow sflowprofile1 remote-endpoint any vlan add 5-10
mac access-group stdmacaclin in
ip access-group stdipaclin in
ipv6 access-group stdipv6aclin in
```

Related Commands

overlay-gateway, show overlay-gateway

show running-config password-attributes

Displays global password attributes.

Syntax

show running-config password-attributes

Modes

Privileged EXEC mode

Usage Guidelines

The attributes will not be displayed when they hold default values.

Examples

To display the global password attributes:

```
switch# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

Related Commands

service password-encryption

show running-config police-priority-map

Displays configured police-priority-maps.

Syntax

show running-config class-map

Modes

Privileged EXEC mode

Usage Guidelines

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples

To display configured police-priority-maps:

```
switch# configure terminal

switch(config)# do show running-config police-priority-map

police-priority-map pmap1
 conform 0 1 1 2 1 2 1 1
 exceed 3 3 3 3 4 5 6 7
```

Related Commands

police-priority-map

show running-config policy-map

Displays the currently running policy-map configurations.

Syntax

show running-config policy-map

Modes

Privileged EXEC mode

Usage Guidelines

Output includes the policy-map name, class-map name, and class-map configuration.

Examples

To currently running policy-maps and their configuration:

```
switch# show running-config policy-map

policy-map policy_map1
 class default
  police cir 50000 cbs 500000 eir 60000 ebs 40000 set-priority prio_map1 conform-set-dscp 23 conform-
set-tc 4 exceed-set-prec 2 exceed-set-tc 5
 !
!
policy-map policy_map2
 class default
  police cir 1000000 cbs 200000
```

Related Commands

class, policy-map, qos cos, show running-config class-map

show running-config port-profile

Displays configured AMPP port-profiles.

Syntax

show running-config port-profile [*name*]

Parameters

name

Specifies the name of a port-profile. If no name is provided, information about all port-profiles is displayed.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config port-profile

port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
```

Related Commands

port-profile (global configuration mode), show port-profile, show running-config port-profile activate, show running-config port-profile fcoe-profile, show running-config port-profile qos-profile, show running-config port-profile security-profile, show running-config port-profile static, show running-config port-profile vlan-profile, show running-config port-profile-domain

show running-config port-profile activate

Displays activated AMPP port-profiles.

Syntax

show running-config port-profile [*name*] **activate**

Parameters

name

Specifies the name of a port-profile. If no name is provided, information about all activated port-profiles is displayed.

Modes

Privileged EXEC mode

Usage Guidelines

This command display port profiles that are activated. These port profiles are available for association with MAC addresses.

Related Commands

port-profile (global configuration mode), show running-config port-profile

show running-config port-profile fcoe-profile

Displays the configured FCOE subprofile.

Syntax

show running-config port-profile [*name*] **fcoe-profile** [**fcoeport** [**default**]]

Parameters

name

Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the FCOE profile applied is displayed.

fcoeport [**default**]

Specifies an FCOE map name. The only map name supported currently is "default."

Modes

Privileged EXEC mode

Related Commands

fcoe, fcoe-profile (AMPP), port-profile (global configuration mode), show running-config port-profile

show running-config port-profile qos-profile

Displays the configured Quality of Service (QoS) subprofile.

Syntax

show running-config port-profile [*name*] **qos-profile** [**cee** [**name**] | **qos** [**cos** *cos* | **cos-mutation** *name* | **cos-traffic-class** *name* | **flowcontrol** [**pfc** | **rx** | **tx**] | **trust** [**cos**]]

Parameters

name
Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the QoS subprofile applied is displayed.

cee [*name*]
The configured QoS CEE map.

qos
The QoS profile.

cos *cos*
The configured default class of service (CoS).

cos-mutation *name*
The applied Cos-to-Cos mutation map.

cos-traffic-class *name*
The applied Cos-to-Traffic class map.

flowcontrol
The configured IEEE 802.3x flow control.

pfc
Whether priority-based flow control (PFC) is enabled.

rx
Whether Pause reception is enabled.

tx
Whether Pause generation is enabled.

trust
The configured QoS trust configuration.

cos
Whether the Layer 2 CoS field in incoming packets is configured as trusted for deriving the internal traffic class.

Modes

Privileged EXEC mode

Related Commands

port-profile (global configuration mode), qos cos, qos cos-mutation, qos flowcontrol pfc, qos flowcontrol, qos map cos-traffic-class, qos-profile (AMPP), security-profile (AMPP), show running-config port-profile

show running-config port-profile security-profile

Displays security subprofiles.

Syntax

show running-config port-profile [*name*] **security-profile** [**mac** [**access-group** [*acl-name* | **in**]]]

Parameters

name

Specifies the name of a port-profile. If no name is provided, information about all port-profiles with the security subprofile applied is displayed.

mac

The configured MAC parameters.

access-group

The applied ACL.

acl-name

Specifies an ACL.

in

Ingress direction.

Modes

Privileged EXEC mode

Related Commands

mac access-group, show running-config port-profile, port-profile (global configuration mode), port-profile-port, security-profile (AMPP)

show running-config port-profile static

Displays statically associated VM MAC addresses and the port profiles with which they are statically associated.

Syntax

show running-config port-profile [*name*] **static** [*mac-address*]

Parameters

name

Specifies the name of a port-profile. If no name is provided, information about all port-profiles associated with VM MAC addresses is displayed.

mac-address

Displays the port-profile associated with a specific MAC address.

Modes

Privileged EXEC mode

Related Commands

port-profile (global configuration mode), show running-config port-profile

show running-config port-profile vlan-profile

Displays information about VLAN subprofiles.

Syntax

show running-config port-profile [*name*] **vlan-profile** [**switchport** [**access** [**vlan** [*vlan_id*]] | **mode** [**access** | **trunk**] | **trunk** [**allowed** [**vlan** [**add** [*vlan_id*] | **all** | **except** *vlan_id* | **none** | **remove** [*vlan_id*]]] | **native-vlan** *vlan_id*]]]

Parameters

name
Specifies the name of a port-profile. If no name is provided, information about all port-profiles with a VLAN subprofile applied is displayed.

switchport
Specifies the configured switching characteristics of the Layer 2 interfaces.

access
Specifies VLAN interfaces for which access is configured for the VLAN profile mode.

vlan *vlan_id*
Specifies a VLAN interface configured for access.

mode
Specifies the configured mode of the Layer 2 interface.

access
Specifies Layer 2 interfaces configured for access mode.

trunk
Specifies Layer 2 interfaces configured for trunk mode.

trunk
Specifies Layer 2 interfaces configured for trunk mode.

allowed
Specifies VLANs that are configured to transmit and receive through the Layer 2 interface.

vlan add [*vlan_id*]
Specifies VLANs that are allowed to transmit and receive through the Layer 2 interface.

vlan all
Specifies all VLANs that are allowed to transmit and receive through the Layer 2 interface.

vlan except *vlan_id*
Specifies VLANs that excepted from transmitting and receiving through the Layer 2 interface.

vlan none
Specifies VLANs that are allowed to transmit and receive through the Layer 2 interface.

vlan remove [*vlan_id*]
Specific VLANs to be removed from those allowed to transmit and receive through the Layer 2 interface.

native-vlan *vlan_id*
Specifies native VLANs configured to classify untagged traffic

Modes

Privileged EXEC mode

Examples

```
switch# show running-config port-profile vlan-profile

port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk native-vlan 1
!
!
switch# show running-config port-profile vlan-profile switchport trunk native-vlan

port-profile default
vlan-profile
switchport trunk native-vlan 1
!
!
```

Related Commands

port-profile (global configuration mode), show running-config port-profile, switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan, vlan-profile (AMPP)

show running-config port-profile-domain

Displays the port-profile domains and their associated port-profiles.

Syntax

show running-config port-profile-domain

Modes

Privileged EXEC mode

Usage Guidelines

```
switch# show running-config port-profile-domain
port-profile-domain PP0
  port-profile pp1
  port-profile pp4
!
port-profile-domain PP1
  port-profile pp3
  port-profile pp4
```

show running-config protocol cdp

Displays the Cisco Discovery Protocol (CDP) information.

Syntax

show running-config protocol cdp

Modes

Privileged EXEC mode

show running-config protocol edge

Displays the Edge Loop Detection (ELD) parameters.

Syntax

show running-config protocol edge { **hello-interval** | **pdu-rx-limit** | **shutdown-time** }

Parameters

hello-interval
Displays the hello-interval-limit value.

pdu-rx-limit
Displays the bpdu-rx-limit value.

shutdown-time
Displays the shutdown-time-limit value.

Modes

Privileged EXEC mode

show running-config protocol lldp

Displays the Link Layer Discovery Protocol (LLDP) parameters.

Syntax

show running-config protocol lldp advertise { { **dcbx-fcoe-app-tlv** | **dcbx-fcoe-logical-link-tlv** | **dcbx-iscsi-app-tlv** | **dcbx-tlv** | **dot1-tlv** | **dot3-tlv** | **optional-tlv** } | **description** | **disable** | **hello** | **iscsi-priority** | **mode** | **multiplier** | **profile** { **description** } | **system-description** | **system-name** }

Parameters

advertise
Displays the Advertise TLV configuration information.

dcbx-fcoe-app-tlv
Displays the IEEE Data Center Bridging eXchange FCoE Application TLV information.

dcbx-fcoe-logical-link-tlv
Displays the IEEE Data Center Bridging eXchange FCoE Logical Link TLV information.

dcbx-iscsi-app-tlv
Displays the IEEE Data Center Bridging eXchange iSCSI Application TLV information.

dcbx-tlv
Displays the IEEE Data Center Bridging eXchange TLV information.

dot1-tlv
Displays the IEEE 802.1 Organizationally Specific TLV information.

dot3-tlv
Displays the IEEE 802.3 Organizationally Specific TLV information.

optional-tlv
Displays the Optional TLVs information.

description
Displays the User description

disable
Displays the Disable LLDP

hello
Displays the Hello Transmit interval.

iscsi-priority
Displays the Ethernet priority to advertise for iSCSI

mode
Displays the LLDP mode.

multiplier
Displays the Timeout Multiplier

profile description
Displays the LLDP Profile table and description.

system-description
Displays the System Description.

system-name
Displays the System Name

Modes

Privileged EXEC mode

show running-config protocol spanning-tree mstp

Displays the protocol configuration information for MSTP.

Syntax

show running-config protocol spanning-tree mstp [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Parameters

bridge-priority
Displays the Bridge priority commands.

cisco-interoperability
Displays the Cisco Interoperability status.

description
Displays the spanning tree description.

error-disable-timeout
Displays the Error-disable-timeout for the spanning tree.

forward-delay
Displays the forward delay for the spanning tree.

hello-time
Displays the hello time settings.

instance
Displays the MST instance.

max-age
Displays the max age for the spanning tree.

max-hops
Displays the MST max hop count.

port-channel
Displays the status of port-channel for spanning-tree.

region
Displays the MST region.

revision
Displays the revision number for configuration information.

shutdown
Displays the status of the spanning-tree protocol.

transmit-holdcount
Displays the current transmit hold count of the bridge.

vlan
Displays the VLAN ID

Modes

Privileged EXEC mode

Related Commands

spanning-tree shutdown

show running-config protocol spanning-tree pvst

Displays the protocol configuration information for PVST.

Syntax

show running-config protocol spanning-tree pvst [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Parameters

bridge-priority
Displays the Bridge priority commands.

description
Displays the spanning tree description.

error-disable-timeout
Displays the Error-disable-timeout for the spanning tree.

forward-delay
Displays the forward delay for the spanning tree.

hello-time
Displays the hello time settings.

max-age
Displays the max age for the spanning tree.

port-channel
Displays the status of port-channel for spanning-tree.

shutdown
Displays the status of the spanning-tree protocol.

vlan
Displays the VLAN ID

Modes

Privileged EXEC mode

Related Commands

spanning-tree shutdown

show running-config protocol spanning-tree rpvst

Displays the protocol configuration information for RPVST.

Syntax

show running-config protocol spanning-tree rpvst [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Parameters

bridge-priority
Displays the Bridge priority commands.

cisco-interoperability
Displays the Cisco Interoperability status.

description
Displays the spanning tree description.

error-disable-timeout
Displays the Error-disable-timeout for the spanning tree.

forward-delay
Displays the forward delay for the spanning tree.

hello-time
Displays the hello time settings.

max-age
Displays the max age for the spanning tree.

port-channel
Displays the status of port-channel for spanning-tree.

shutdown
Displays the status of the spanning-tree protocol.

transmit-holdcount
Displays the current transmit hold count of the bridge.

vlan
Displays the VLAN ID

Modes

Privileged EXEC mode

Related Commands

spanning-tree shutdown

show running-config protocol spanning-tree rstp

Displays the protocol configuration information for RSTP.

Syntax

show running-config protocol spanning-tree rstp [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Parameters

bridge-priority
Displays the Bridge priority commands.

description
Displays the spanning tree description.

error-disable-timeout
Displays the Error-disable-timeout for the spanning tree.

forward-delay
Displays the forward delay for the spanning tree.

hello-time
Displays the hello time settings.

max-age
Displays the max age for the spanning tree.

port-channel
Displays the status of port-channel for spanning-tree.

shutdown
Displays the status of the spanning-tree protocol.

transmit-holdcount
Displays the current transmit hold count of the bridge.

Modes

Privileged EXEC mode

Related Commands

spanning-tree shutdown

show running-config protocol spanning-tree stp

Displays the protocol configuration information for STP.

Syntax

show running-config protocol spanning-tree stp [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Parameters

bridge-priority
Displays the Bridge priority commands.

description
Displays the spanning tree description.

error-disable-timeout
Displays the Error-disable-timeout for the spanning tree.

forward-delay
Displays the forward delay for the spanning tree.

hello-time
Displays the hello time settings.

max-age
Displays the max age for the spanning tree.

port-channel
Displays the status of port-channel for spanning-tree.

shutdown
Displays the status of the spanning-tree protocol.

Modes

Privileged EXEC mode

Related Commands

spanning-tree shutdown

show running-config protocol udld

Displays the UDLD global parameters.

Syntax

show running-config protocol udld advertise { **hello** | **multiplier** | **shutdown** }

Command Default

This command has no defaults.

Parameters

hello
Displays the Hello Transmit interval.

multiplier
Displays the Timeout Multiplier.

shutdown
Displays the shutdown status.

Modes

Privileged EXEC mode

show running-config radius-server

Displays the local switch configuration for the RADIUS server from the configuration database.

Syntax

show running-config radius-server host { *ip-address* | *hostname* }

Parameters

host

Identifies the RADIUS server by host name or IP address.

hostname

Specifies the host name of the RADIUS server.

ip-address

Specifies the IP address of the RADIUS server. IPv4 and IPv6 are supported.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config radius-server host 10.38.37.180

radius-server host 10.38.37.180
protocol   pap
key          changedsec
timeout    3
```

Related Commands

radius-server, show running-config tacacs-server, tacacs-server

show running-config rbridge-id

Displays configuration for the RBridge ID.

Syntax

show running-config rbridge-id *rbridge-id* [**fcoe**]

Parameters

rbridge-id

Specifies an RBridge ID.

fcoe

Displays the FCoE information for the RBridge ID.

Modes

Privileged EXEC mode

Examples

```
switch# show running-config rbridge-id 2

rbridge-id 2
 interface-nodespecific ns-vlan 10
 interface-nodespecific ns-ethernet 100
 fabric vlag 10 load-balance src-dst-mac-vid
 fabric vlag 20 load-balance dst-mac-vid
 no protocol vrrp

switch# show running-config rbridge-id 21 fcoe
rbridge-id 21
 fcoe
  fcoe-enodes 1000
```

Related Commands

show fabric ecmp load-balance

show running-config rbridge-id hardware-profile

Displays the route table and TCAM profiles in the running configuration for all RBridge IDs or a specified RBridge ID.

Syntax

show running-config rbridge-id [*rbridge-id*] **hardware-profile** [**route-table** [**default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd**] | **tcam** [**default** | **ipv4-max-route** | **ipv4-max-arp** | **ipv4-min-v6** | **ipv6-max-route** | **ipv6-max-nd**]]

Parameters

rbridge-id

Specifies an RBridge ID or all RBridge IDs.

rbridge-id

Range is from 1 through 239. This option is available only in logical chassis cluster mode.

route-table

Specifies hardware resources for route profiles.

default

Specifies IPv4/IPv6 resources for dual-stack operations.

ipv4-max-route

Specifies resources for the maximum number of IPv4 routes.

ipv4-max-arp

Specifies resources for the maximum number of IPv4 ARP entries.

ipv4-min-v6

Specifies resources for IPv4 routes in dual-stack configurations.

ipv6-max-route

Specifies resources for the maximum number of IPv6 routes.

ipv6-max-nd

Specifies resources for the maximum number of IPv6 Neighbor Discovery entries.

tcam

Specifies hardware resources for TCAM profiles.

default

Specifies resources with basic support for all applications.

l2-ipv4-acl

Specifies resources for Layer 2 and IPv4 ACLs.

ipv4-v6-pbr

Specifies resources for IPv4 and IPv6 ACLs and policy-based routing tables.

ipv4-v6-qos

Specifies resources for IPv4 and IPv6 ACLs and QoS.

ipv4-v6-mcast

Specifies resources for multicast.

l2-acl-qos
Specifies resources for Layer 2 ACLs and QoS.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

Examples

The following shows the use of the **show running-config rbridge-id hardware-profile** command, without the specification of an RBridge ID, to display the results of the configuration on the local switch. You can also specify an RBridge ID.

```
switch# show running-config rbridge-id hardware-profile
rbridge-id 11
 hardware-profile tcam ipv4-v6-mcast
 hardware-profile route-table ipv6-max-nd
!
rbridge-id 12
 hardware-profile tcam l2-ipv4-acl
 hardware-profile route-table ipv4-max-arp
```

show running-config rbridge-id linecard

Displays the line card configuration.

Syntax

show running-config rbridge-id *rbridge-id* **linecard**

Parameters

rbridge-id

Specifies an RBridge ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command must be executed in the current RBridge ID context.

Examples

To display the line card configuration for the local switch:

```
switch# show running-config rbridge-id 1 linecard

rbridge-id 1
 linecard 1 LC48x10G
 linecard 2 LC48x10G
 linecard 3 LC12x40G
 linecard 4 LC48x10G
```

Related Commands

linecard

show running-config rbridge-id ssh

Displays the Secure Shell (SSH) configuration for an RBridge ID.

Syntax

show running-config rbridge-id *rbridge-id* **ssh**

Parameters

rbridge-id
Specifies an RBridge ID.

Modes

Privileged EXEC mode

show running-config rmon

Displays Remote Monitor configuration information.

Syntax

show running-config rmon [**alarm** | **event**]

Parameters

alarm

Displays the Remote Monitor alarm configuration.

event

Displays the Remote Monitor event configuration

Modes

Privileged EXEC mode

Related Commands

rmon alarm, rmon event

show running-config role

Displays the configured roles.

Syntax

show running-config role [**name** *role_name*]

Parameters

name *role_name*

Specifies role assigned to the user.

Modes

Privileged EXEC mode

Examples

To display the roles configured on the switch:

```
switch# show running-config role

role name VLANAdmin desc "Manages security CLIs"
role name NetworkAdmin desc "Manages Network CLIs"
role name ClusterAdmin desc "Manages Cluster CLIs"
```

Related Commands

role name, rule, show running-config rule

show running-config route-map

Displays the status of a route-map application on the specified interface.

Syntax

show running-config route-map [*name*]

Parameters

name

Specifies the name of the route-map.

Modes

Privileged EXEC mode

Usage Guidelines

There is no need to specify the route map name as the user is only allowed to apply a single route map to an interface.

Examples

```
sw0# show running-config route-map abc
ip policy route-map abc permit 20
   match ip address acl Vincent
   set ip vrf pulp_fiction next-hop 3.3.3.5
   set ip next-hop 4.4.4.4switch#
```

Related Commands

route-map

show running-config rule

Displays configured access rules.

Syntax

show running-config rule [*index*] [{ **action** { **reject** | **accept** } | **command** *command_name* | **operation** { **read-only** | **read-write** } | **role** *role_number* }]

Parameters

rule
Displays all configured rules

index
Displays the rule with the specified index number. The valid range is from 1 through 512.

action { **reject** | **accept** }
Displays all rules with the specified action: accept or reject.

command *command_name*
Displays all rules for the specified command. Type a question mark (?) to display a list of valid commands.

operation { **read-only** | **read-write** }
Displays the operation for the command.

role *role_number*
Displays all rules for the specified role.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command without parameters to display rules that have been defined and associated with a particular role.

Examples

To display the configured roles and their access rules:

```
switch# show running-config rule

rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role
!
rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule
!
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
!
rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa
!
rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server
!
rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
!
rule 40 action accept operation read-write role FCOEAdmin
rule 40 command "interface fcoe"
```

To display a single rule:

```
switch# show running-config rule 30

rule 30
 action accept operation read-write role NetworkSecurityAdmin
 command role
```

Related Commands

role name, rule, show running-config role

show running-config secpolicy

Displays the Switch Connection Control (SCC) security policy information.

Syntax

show running-config [**rbridge-id** { *rbridge-id* | **all** }] **secpolicy** { **defined-policy** | **active-policy** }

Parameters

defined-policy
Displays the defined policy and its policy member set.

active-policy
Displays the active policy and its policy member set.

rbridge-id
Specifies an RBridge or all RBridges.

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the active policy and the defined policy and its policy member set.

The **rbridge-id** parameter is supported in VCS mode only.

Examples

To show only the defined policy of rbridge-id 3:

```
switch# show running-config rbridge-id 3 secpolicy defined-policy
rbridge-id 3
secpolicy defined-policy SCC_POLICY
 member-entry aa:aa:aa:aa:aa:aa:aa:aa
 !
 member-entry bb:bb:bb:bb:bb:bb:bb:bb
 !
 member-entry cc:cc:cc:cc:cc:cc:cc:cc
 !
!
switch#
```

To show only the active policy of rbridge-id 3:

```
switch# show running-config rbridge-id 3 secpolicy active-policy
rbridge-id 3
secpolicy active-policy SCC_POLICY
 member-entry aa:aa:aa:aa:aa:aa:aa:aa
 !
 member-entry bb:bb:bb:bb:bb:bb:bb:bb
 !
 member-entry cc:cc:cc:cc:cc:cc:cc:cc
 !
!
switch#
```

To show both active and defined policies of rbridge-id 3:

```
switch# show running-config rbridge-id 3 secpolicy
rbridge-id 3
secpolicy defined-policy SCC_POLICY
 member-entry aa:aa:aa:aa:aa:aa:aa:aa
 !
 member-entry bb:bb:bb:bb:bb:bb:bb:bb
 !
 member-entry cc:cc:cc:cc:cc:cc:cc:cc
 !
!
secpolicy active-policy SCC_POLICY
 member-entry aa:aa:aa:aa:aa:aa:aa:aa
 !
 member-entry bb:bb:bb:bb:bb:bb:bb:bb
 !
 member-entry cc:cc:cc:cc:cc:cc:cc:cc
```

Related Commands

secpolicy activate, secpolicy defined-policy

show running-config sflow

Displays the IPv4 and IPv6 addresses and ports of sFlow collectors.

Syntax

show running-config sflow

Modes

Privileged EXEC mode

Examples

To display the IPv4 and IPv6 addresses and ports of sFlow collectors:

```
switch# show running-config sflow
Sflow collector               3ffe:1900:4545:3:200:f8ff:fe21:67cf : 6343
Sflow collector               fe80::200:f8ff:fe21:67cf     : 6343
Sflow collector            192.35.41.32 : 6343
```

show running-config sflow-policy

Displays the configured sFlow policies.

Syntax

show running-config sflow-policy

Modes

Privileged EXEC mode

Examples

To display the configured sFlow policies.

```
switch# show running-config sflow-policy
```

show running-config sflow-profile

Displays the configured sFlow policies.

Syntax

show running-config sflow-profile

Modes

Privileged EXEC mode

show running-config snmp-server

Shows the running configuration of the SNMP server on the switch.

Syntax

show running-config snmp-server

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the current SNMP configurations of host, community, contact, user, and location.

This command has no default configurations.

Examples

The following command shows the running configuration of the SNMP server on the switch, with encryption applied:

```
switch# show running-config snmp-server

snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 10.17.37.107 public
snmp-server user snmp
snmp-server user snmpadmin1 groupname snmpadmin auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n"
priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n"
priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser2
snmp-server user snmpuser3 auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password
"ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
```

Related Commands

snmp-server community, snmp-server contact, snmp-server context, snmp-server engineid local, snmp-server group, snmp-server host, snmp-server location, snmp-server sys-descr, snmp-server user, snmp-server v3host, snmp-server view

show running-config snmp-server engineid

Shows the engine ID of the SNMP server on the switch.

Syntax

show running-config snmp-server engineid

Modes

Privileged EXEC mode

Examples

To see the engine ID of the SNMP server:

```
switch# show running-config rbridge-id 1 snmp-server engineID local 10:20:30:40:50:60:70:80:90:10:30:12
```

Related Commands

snmp-server community, snmp-server contact, snmp-server context, snmp-server engineid local, snmp-server group, snmp-server host, snmp-server location, snmp-server sys-descr, snmp-server user, snmp-server v3host, snmp-server view

show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

Syntax

show running-config ssh

Modes

Privileged EXEC mode

show running-config ssh server

Displays the SSH server status in the running-config.

Syntax

show running-config [**rbridge-id** { *rbridge-id* | **all** }] **ssh server**

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

SSH server configuration is placed at the beginning of the running-config and is part of the global configuration of the switch. SSH is enabled by default and no entry is shown in the running-config when set to default.

Examples

When SSH service is shut down:

```
switch# show running-config rbridge-id 3 ssh server
rbridge-id 3
ssh server shutdown
switch# show running-config rbridge-id 3 ssh server
rbridge-id 3
ssh server shutdown
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange is configured to DH Group 14:

```
switch# show running-config rbridge-id 3 ssh server key-exchange
rbridge-id 3
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
switch# show running-config rbridge-id 3 ssh server key-exchange
rbridge-id 3
```

When SSH service is enabled:

```
switch# show running-config [rbridge-id
rbridge-id
 | all] ssh server
% No entries found
```

Related Commands

show ssh server status, ssh server shutdown

show running-config ssh server key-exchange

Displays the SSH server key-exchange status in the running-config.

Syntax

show running-config ssh server key-exchange

Modes

Privileged EXEC mode

Examples

Typical command output:

```
switch# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

Related Commands

show ssh server status

show running-config support

Displays the support parameters in the running configuration.

Syntax

show running-config support [**ffdc**]

Parameters

ffdc

Displays the FFDC settings.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display the support parameters in the running configuration:

```
switch# show running-config support ffdc
support ffdc
switch#
```

Related Commands

show support, telnet server shutdown

show running-config support autoupload-param

Displays autoupload parameters.

Syntax

show running-config support autoupload-param

Modes

Privileged EXEC mode

Examples

```
switch(config)# do show running-config support autoupload-param
support autoupload-param hostip 10.31.2.27 username hegdes directory /users/home40/hegdes/autoupload
protocol ftp password "3iTYxJWEUHp9axZQt2tbvw==\n"
switch(config)#
```

show running-config support support-param

Displays support parameters

Syntax

show running-config support support-param [**hostip** *host-ip* **user** *user_acct* **password** *password* **protocol** [**ftp** | **scp** | **sftp**] **directory** *path*]

Parameters

hostip *host-ip*
Displays the IP address of the remote host.

user *user_acct*
Displays the user name to access the remote host.

password *password*
Displays the password to access the remote host.

protocol FTP | SCP | SFTP
Displays the protocol used to access the remote server.

directory *path*
Displays the path to the directory.

Modes

Privileged EXEC mode

Examples

```
switch(config)# do show running-config support support-param
support support-param hostip 10.31.2.27 username hegdes directory /users/home40/hegdes/support protocol
ftp password "3iTYxJWEUHp9axZQt2tbvw==\n"
switch(config)#
```

History

Release version	Command history
5.0.0	This command was introduced.

show running-config switch-attributes

Displays switch attributes.

Syntax

show running-config switch-attributes [*rbridge-id*] { **chassis-name** | **host-name** }

Command Default

Displays all switch attributes on the local switch.The default host name is "sw0". The default chassis name depends on the switch model.

Parameters

rbridge-id
Specifies an RBridge ID.

chassis-name
Displays the switch chassis name.

host-name
Displays the switch host name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To display all attributes for the local switch:

```
switch# show running-config switch-attributes

switch-attributes 2
 chassis-name VDX6740-48
 host-name sw0
!
```

To display the host name of the local switch:

```
switch# show running-config switch-attributes host-name

switch-attributes 2
 host-name sw0
!
```

Related Commands

switch-attributes

show running-config system-monitor

Displays the system monitor configuration.

Syntax

show running-config system-monitor [**fan** | **power** | **temp** | **cid-card** | **sfp** | **compact-flash** | **MM** | **LineCard** | **SFM**]

Parameters

fan
Displays the threshold and alert setting for the FAN component.

power
Displays the threshold and alert setting for the power component.

temp
Displays the threshold for the temperature sensor component.

cid-card
Displays the threshold for the CID card component.

sfp
Displays the threshold for the small form factor pluggable (SFP) device.

compact-flash
Displays the threshold for the compact flash device.

MM
Displays the threshold for the management module.

LineCard
Displays the threshold for the line card.

SFM
Displays the threshold for the switch fabric module.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

```
switch# show running-config system-monitor

system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 0 down-threshold 1
system-monitor power alert state removed action raslog
system-monitor temp threshold marginal-threshold 1 down-threshold 2
system-monitor cid-card threshold marginal-threshold 1 down-threshold 0
system-monitor cid-card alert state inserted,faulty action email
system-monitor sfp alert state none action none
system-monitor compact-flash threshold marginal-threshold 1 down-threshold 0
system-monitor MM threshold marginal-threshold 1 down-threshold 0
system-monitor LineCard threshold marginal-threshold 1 down-threshold 0
system-monitor LineCard alert state removed action raslog
system-monitor SFM threshold marginal-threshold 1 down-threshold 0
```

Related Commands

show system monitor, system-monitor-mail

show running-config system-monitor-mail

Displays the system monitor mail configuration.

Syntax

show running-config system-monitor-mail { **fru enable** }

Parameters

fru

Displays FRU information.

enable

Displays the status of the FRU.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Related Commands

show system monitor, system-monitor-mail

show running-config tacacs-server

Displays the TACACS+ server configuration.

Syntax

show running-config tacacs-server [**host** *ipaddr* | *hostname*]

Parameters

host

Identifies the TACACS+ server by host name or IP address.

ipaddr

Specifies the IP address of the TACACS+ server (IPv4 or IPv6).

hostname

Specifies the domain name of the TACACS+ server.

source-ip [*chassis-ip* | *mm-ip*]

Specifies the chassis IP address or MM IP address as the source IP address for TACACS+ authentication and accounting.

Modes

Privileged EXEC mode

Examples

To display the list of configured TACACS+ servers:

```
switch# show running-config tacacs-server host
fec0:60:69bc:94:211:25ff:fec4:6010
```

To display a single IPv4 TACACS+ server configuration:

```
switch# show running-config tacacs-server host 10.24.65.6
```

To display a single IPv5 TACACS+ server configuration:

```
switch# show running-config tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
```

Related Commands

radius-server, show running-config radius-server, tacacs-server

show running-config telnet server

Displays the Telnet server status in the running-config.

Syntax

show running-config [**rbridge-id** { *rbridge-id* | **all** }] **telnet server**

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Telnet server configuration is placed at the beginning of running-config and is part of the global configuration of the switch. Telnet is enabled by default and there will be no entry in the running-config when set to default.

Examples

When Telnet service is shut down:

```
switch# show running-config rbridge-id 3 telnet server
rbridge-id 3
telnet server shutdown
```

When Telnet service is enabled:

```
switch# show running-config [rbridge-id
rbridge-id
 | all] telnet server
% No entries found
```

Related Commands

show telnet server status, telnet, telnet server shutdown

show running-config threshold-monitor

Displays the system's threshold configuration.

Syntax

show running-config threshold-monitor

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

```
switch# show running-config threshold-monitor

threshold-monitor Cpu poll 30 retry 2 limit 60 actions raslog
threshold-monitor Memory poll 30 retry 2 limit 70 high-limit low-limit 50 actions none
switch# show running-config threshold-monitor area IFG

Interface                          Area       Value  Status        Monitoring
                                                                     Status
---------                    ----------------  ------ -------     ------------
fortygigabitethernet 3/8     IFG Violation Error  30  Out of Range  Monitoring
fortygigabitethernet 3/9     IFG Violation Error   0  In Range      Monitoring
<All other online interfaces> IFG Violation Error   0  In Range      Monitoring
```

Related Commands

show system monitor, system-monitor-mail

show running-config threshold-monitor interface

Displays the system's running interface configuration.

Syntax

show running-config threshold-monitor interface

Modes

Privileged EXEC mode

Usage Guidelines

Default values are not displayed under the **show running-config threshold-monitor interface** command. Only custom values are displayed.

Examples

```
switch# do show running-config threshold-monitor interface

switch(config)# do show running-config threshold-monitor interface
threshold-monitor interface apply custom-monitoring
threshold-monitor interface pause
threshold-monitor interface policy  custom type Ethernet area MissingTerminationCharacter threshold
timebase minute high-threshold 20 low-threshold 1 buffer 5
threshold-monitor interface policy custom type Ethernet area MissingTerminationCharacter alert above
highthresh-action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area MissingTerminationCharacter alert below
highthresh-action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area CRCAlignErrors threshold timebase hour
high-threshold 80 low-threshold 10 buffer 35
threshold-monitor interfacepolicy  custom type Ethernet area CRCAlignErrors alert above highthresh-
action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area CRCAlignErrors alert below highthresh-
action none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area SymbolErrors threshold timebase minute
high-threshold 20 low-threshold 1 buffer 5
threshold-monitor interfacepolicy custom type Ethernet area SymbolErrors alert above highthresh-action
none lowthresh-action none
threshold-monitor interface policy custom type Ethernet area SymbolErrors alert below highthresh-action
none lowthresh-action none
threshold-monitor interface policy  custom type Ethernet area IFG threshold timebase minute high-
threshold 20 low-threshold 1 buffer 5
threshold-monitor interface policy custom type Ethernet area IFG alert above highthresh-action
raslog,portfence lowthresh-action emailraslog
threshold-monitor interface policy custom type Ethernet area IFG alert below highthresh-action none
lowthresh-action none
```

Related Commands

show system monitor

show running-config threshold-monitor security

Displays the system's running security configuration.

Syntax

show running-config threshold-monitor security

Modes

Privileged EXEC mode

Usage Guidelines

Default values are not displayed under the **show running-config threshold-monitor security** command. Only custom values are displayed.

Examples

```
switch# show running-config threshold-monitor security policy custom area telnet-violation

threshold-monitor security policy custom area telnet-violation timebase hour
threshold-monitor security policy custom area telnet-violation threshold thresh_high high-threshold 10
buffer 20
switch# show running-config threshold-monitor policy custom area login-violation
threshold-monitor securitym policy custom area login-violation alert above highthresh_action all
threshold-monitor security apply custom
switch#
```

Related Commands

show system monitor

show running-config threshold-monitor sfp

Displays the system's running SFP configuration.

Syntax

show running-config threshold-monitor sfp

Modes

Privileged EXEC mode

Usage Guidelines

Default values are not displayed under the **show running-config threshold-monitor sfp** command. Only custom values are displayed.

Examples

```
switch# do show running-config threshold-monitor sfp

threshold-monitor sfp pause
threshold-monitor sfp apply custom
threshold-monitor sfp policy custom Type 1GSR area TXP threshold high-threshold 2000 low-threshold 1000
buffer 500
threshold-monitor sfp policy custom Type 1GSR area TXP alert above highthresh-action raslog lowthresh-
action none
threshold-monitor sfp policy custom Type 1GSR area TXP alert below highthresh-action none lowthresh-
action raslog
```

Related Commands

show system monitor

show running-config username

Displays the user accounts on the switch.

Syntax

show running-config *username* [[**username**] [**desc**] [**enable**] [**encryption-level**] [**password**] [**role**]]

Parameters

username
The account name associated with the user. The maximum number of characters is 40.

desc
Displays the description of the user configuration.

enable
Displays the account status: enable true = enabled (default) enable false = disabled

encryption-level
Password encryption level. Values are 0 through 7. The default is 0.

password
Account password.

role
The role associated with the account.

Modes

Privileged EXEC mode

Usage Guidelines

When used without operands, Use this command to display all user accounts on the switch.

Use the various parameters to query the specified account details.

This command does not display the root account.

Defaults are not displayed.

Examples

To display the user accounts on the switch:

```
switch# show running-config username

username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role user desc User
```

To display a specific user account:

```
switch# show running-config username admin

username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
```

To display the enabled status for a specific user account

```
switch# show running-config username admin enable

username admin enable true
```

Related Commands

show users, unlock username, username

show running-config vcs

Displays VCS configuration information.

Syntax

show running-config vcs [**virtual** [**ip** [**address**]]]

Parameters

virtual
Displays the VCS configuration.

ip
Displays the virtual IP configuration.

address
Displays the virtual IP address.

Modes

Privileged EXEC mode

Related Commands

vcs config snapshot (logical chassis cluster mode)

show running-config zoning

Displays the zoning configuration.

Syntax

show running-config zoning [**defined-configuration** | **enabled-configuration**]

Parameters

defined-configuration
Displays the defined configuration parameters. See **show running-config zoning defined-configuration**.

enabled-configuration
Displays the enabled configuration parameters. See **show running-config zoning enabled-configuration**.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the zoning configuration for a Brocade VCS Fabric. The base command lists both the defined and the enabled configuration.

This command is supported in VCS mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

To display the enabled-configuration enabled-zone information, use the **show zoning enabled-configuration** command.

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples

The following example displays the zoning configuration:

```
switch# show running-config zoning
zoning defined-configuration cfg cfg1
 member-zone zone1
 member-zone zone2
```

Related Commands

show running-config zoning defined-configuration, show running-config zoning enabled-configuration, show zoning enabled-configuration

show running-config zoning defined-configuration

Displays the defined zone configuration.

Syntax

show running-config zoning defined-configuration

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the zoning configuration for a Brocade VCS Fabric. The base command lists both the defined and a small subset of the enabled configuration.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples

The following example displays the defined zoning configuration:

```
switch# show running-config zoning defined-configuration

zoning defined-configuration cfg cfg0
 member-zone zone_0_1
 member-zone zone_0_2
 member-zone zone_0_3
 member-zone zone_0_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg1
 member-zone zone_1_1
 member-zone zone_1_2
 member-zone zone_1_3
 member-zone zone_1_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg2
 member-zone zone_2_1
 member-zone zone_2_2
 member-zone zone_2_3
 member-zone zone_2_4
 member-zone zone_same
!
zoning defined-configuration cfg cfg4
 member-zone zone2
 member-zone zone3
!
zoning defined-configuration zone zone0
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry 11:22:33:44:55:66:77:82
 member-entry 11:22:33:44:55:66:77:83
 member-entry 11:22:33:44:55:66:77:84
!
zoning defined-configuration zone zone1
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry alias1
 member-entry alias2
 member-entry alias3
!
zoning defined-configuration zone zone2
 member-entry 11:22:33:44:55:66:77:80
 member-entry 11:22:33:44:55:66:77:81
 member-entry 11:22:33:44:55:66:77:82
 member-entry 11:22:33:44:55:66:77:83
 member-entry 11:22:33:44:55:66:77:84
!
```

Related Commands

show running-config zoning, show running-config zoning enabled-configuration

show running-config zoning enabled-configuration

Displays the enabled zone configuration.

Syntax

show running-config zoning enabled-configuration [**cfg-action** | **cfg-name** | **default-zone-access**]

Parameters

cfg-action
Displays the enabled configuration action.

cfg-name
Displays the enabled configuration name.

default-zone-access
Displays the default-zone access mode.

Modes

Privileged EXEC mode

Usage Guidelines

The enabled configuration is the single zone configuration that is currently enabled in a Brocade VCS Fabric. The devices an initiator can access in the network are based on this configuration. The enabled configuration is built when a specific zone configuration is enabled and all error checking has been completed successfully. Use this command to display the name of the enabled zoning configuration, the configuration action, and the default-zone access mode.

The configuration name is displayed differently depending on two main factors:

- If no transaction is pending, the configuration action is set to "cfg-save."
- If a transaction is pending, the configuration name is marked with a CFG_MARKER asterisk (*) and the configuration action is set to "cfg-None" The CFG_MARKER flag can also indicate that the enabled configuration does not exactly match the defined configuration. This scenario occurs when you have an enabled configuration and make edits to the defined configuration, and then, instead of enabling the defined configuration, you issue the cfg-save command.

Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be executed on any RBridge in a Brocade VCS Fabric.

To view details about the enabled zones, use the **show zoning enabled-configuration** command.

Examples

To display the enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration

zoning enabled-configuration cfg-name cfg1
zoning enabled-configuration default-zone-access noaccess
zoning enabled-configuration cfg-action cfg-save
```

To display only the default-zone access mode for the enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration default-zone-access

zoning enabled-configuration default-zone-access allaccess
```

Related Commands

show running-config zoning, show running-config zoning defined-configuration, show zoning enabled-configuration

show secpolicy

Displays the Switch Connection Control (SCC) security policy information.

Syntax

show running-config secpolicy { **defined-policy** | **active-policy** }

Parameters

defined-policy
Displays the defined policy and its policy member set.

active-policy
Displays the active policy and its policy member set.

Modes

Privileged EXEC mode

Examples

To show only the defined policy

```
switch# show running-config secpolicy defined-policy

secpolicy defined-policy SCC_POLICY
member-entry 11:11:11:11:11:11:11:11
!
member-entry 22:22:22:22:22:22:22:22
!
member-entry 33:33:33:33:33:33:33:33
```

To show only the active policy

```
switch# show running-config secpolicy active-policy

secpolicy active-policy SCC_POLICY
member-entry 11:11:11:11:11:11:11:11
!
member-entry 22:22:22:22:22:22:22:22
!
member-entry 33:33:33:33:33:33:33:33
```

To show both active and defined policy

```
switch# show running-config secpolicy

secpolicy defined-policy SCC_POLICY
member-entry 11:11:11:11:11:11:11:11
!
member-entry 22:22:22:22:22:22:22:22
!
member-entry 33:33:33:33:33:33:33:33
!
!
secpolicy active-policy SCC_POLICY
member-entry 11:11:11:11:11:11:11:11
!
member-entry 22:22:22:22:22:22:22:22
!
member-entry 33:33:33:33:33:33:33:33
```

Related Commands

secpolicy activate, secpolicy defined-policy

show sflow

Displays sFlow configuration information and statistics.

Syntax

show sflow [**interface** { *<N>***gigabitethernet** *rbridge-id/slot/port* | **all**

Command Default

sFlow is disabled on all interfaces.

Parameters

all

Displays all sFlow information and statistics.

interface

Displays sFlow information for an Ethernet interface.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

To display sFlow statistics on the 10-gigabit Ethernet interface 15/0/4:

```
switch# show sflow interface tengigabitethernet 15/0/4

sFlow info for interface Ten Gigabit Ethernet 15/0/4
------------------------------------------------
Configured sampling rate:                  100 pkts
Actual sampling rate:                      100 pkts
Counter polling interval:                  100 secs
Samples received from hardware:        32
Port backoffThreshold :                    272
Counter samples collected :                147
```

To display sFlow statistics on 1-gigabit Ethernet interface 22/0/1:

```
switch# show sflow interface gigabitethernet 22/0/1

--------------------------------------------------
sFlow info for interface Gigabit Ethernet 22/0/1
Configured sampling rate:              32768 pkts
Actual sampling rate:                  32768 pkts
Counter polling interval:              20 seconds
Samples received from hardware:        0
Port backoff threshold:                48
--------------------------------------------------
```

To display all sFlow statistics:

```
switch# show sflow all
sFlow services are:                                  enabled
Global default sampling rate:                        32768 pkts
Global default counter polling interval:           20 secs
Collector server address                               Number of samples sent
------------------------                                ----------    -------------
3ffe:1900:4545:3:200:f8ff:fe21:67cf : 6343               0
fe80::200:f8ff:fe21:67cf     : 6343                            0
192.35.41.32    : 6343                                        0
fe80::201:fdff:fe21:43cd     : 6343                           0
192.44.23.45    : 6343                                         0
```

show sflow-profile

Displays the sflow profile configurations.

Syntax

show sflow-profile { *string* | **all** }

Parameters

string

Specifies the name of the profile.

all

Displays all profile information.

Modes

Privileged EXEC mode

Related Commands

sflow enable (global version)

show sfm

Displays information about the switch fabric modules present in the chassis.

Syntax

show sfm

Modes

Privileged EXEC mode

Command Output

The **show sfm** command displays the following information:

Output field	Description
Slot	Displays the slot number. Slots for switch fabric modules are S1 through S3 for Brocade VDX 8770-4 switches and S1 through S6 for Brocade VDX 8770-8 switches.
Type	Displays the interface module type. The switch fabric module type is SFM.
Description	Module description
ID	Displays the module ID. The ID for the switch fabric module is 113.
Status	Displays the status of the module as one of the following: • VACANT - The slot is empty. • POWERED-OF - The module is present in the slot but is powered off. • POWERING UP - The module is present and powering on. • LOADING - The module is present, powered on, and loading the initial configuration. • DIAG RUNNING POST1 - The module is present, powered on, and running the POST (power-on self-test). • DIAG RUNNING POST2 - The module is present, powered on, and running the reboot power on self tests. • INITIALIZING - The module is present, powered on, and initializing hardware components. • ENABLED - The module is on and fully enabled. • DISABLED - The module is powered on but disabled. • FAULTY - The module is faulty because an error was detected. • UNKNOWN -The module is inserted but its state cannot be determined.

Examples

To display the switch fabric modules present in a Brocade VDX 8770-4 chassis:

```
switch# show sfm

Slot  Type         Description                 ID      Status
-------------------------------------------------------------------
 S1   SFM          Switch Fabric Module        113     ENABLED#
 S2   SFM          Switch Fabric Module        113     ENABLED#
 S3   SFM          Switch Fabric Module        113     ENABLED
 # = At least one enabled SFM in these slots is required.
```

Related Commands

show linecard, show mm, show slots

show sfp

Displays the SFP breakout configurations.

Syntax

show sfp [**linecard** *linecard* [**port** *port*]]

Command Default

Displays the SFP breakout information using a line card. Port number is optional. If absent, all SFP port configurations are shown.

Parameters

linecard *linecard*

Specifies line card information.

port *port*

Specifies port information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the SFP configuration for the specified line cards. The speed column shows the breakout speed in breakout mode, and the aggregate speed when not in breakout mode.

This command is supported on the line cards.

Examples

To display the SFP configuration on a line card:

```
switch# show sfp linecard 1
Port      Type          Breakout              Speed
-----------------------------------------------------------------------
1         SFP        n/a                10G
2         QSFP       4x10G              10G
3         SFP        n/a                40G
4         CSFP       10x10G            100G
switch# show sfp linecard 1 port 2
Port      Type         Breakout               Speed
-----------------------------------------------------------------------
2         QSFP      4X10G               10G
```

Related Commands

clear support, copy support, power-off linecard, power-on linecard, show support, show running-config hardware connector

show slots

Displays information about the modules present in the chassis.

Command Output

The **show slots** command displays the following information:

Output field	Description
Slot	Displays the slot number. Slots for interface modules are L1 through L4 on Brocade VDX 8770-4 switches, and L1 through L8 on the Brocade VDX 8770-8 switches.
Type	Displays the module type. Examples are: • MM Management Module • SFM Switch Fabric Module • LC48X10G 48-port 10 GbE interface module (line card) • LC48X1G 48-port 1 GbE interface module • LC12X40G 12-port 40 GbE interface module • 27x40G 27-port 40 GbE interface module • 6x100G 6-port 100 GbE interface module
Description	Module description
ID	Module ID. Examples are: • 112 Management Module • 113 Switch Fabric Module • 114 48-port 10GbE interface module • 127 12-port 10 GbE interface module
Status	Displays the status of the module as one of the following: • VACANT - The slot is empty. • POWERED-OFF - The module is present in the slot but is powered off. • POWERING UP - The module is present and powering on. • LOADING - The module is present, powered on, and loading the initial configuration. • DIAG RUNNING POST1 - The module is present, powered on, and running the POST (power-on self-test). This status is not valid for the management modules. • DIAG RUNNING POST2 - The module is present, powered on, and running the reboot power on self tests. This status is not valid for the management modules. • INITIALIZING - The module is present, powered on, and initializing hardware components. • ENABLED - The module is on and fully enabled. • DISABLED - The module is powered on but disabled. • FAULTY - The module is faulty because an error was detected. • UNKNOWN - The module is inserted but its state cannot be determined.

Syntax

show slots

Modes

Privileged EXEC mode

Examples

To display the modules present in a Brocade VDX 8770-4 chassis:

```
switch# show slots

Slot  Type         Description                 ID      Status
--------------------------------------------------------------------
 M1   MM           Management Module           112     ENABLED
 M2                                                    VACANT
 S1                                                    VACANT#
 S2   SFM          Switch Fabric Module        113     ENABLED#
 S3                                                    VACANT
 L1   LC48X10G     48-port 10GE card           114     ENABLED
 L2   LC48X10G     48-port 10GE card           114     ENABLED
 L3                                                    VACANT
 L4   LC48X1G      48-port 1GE card            131     ENABLED
 # = At least one enabled SFM in these slots is required.
```

NOTE

An "@" following an SFM status line indicates that the status of the optical switch is "OPEN."

Related Commands

show linecard, show sfm

show span path

Displays the SPAN path information.

Syntax

show span path session *session_number*

Parameters

session *session_number*

The path for the SPAN session to display.

Modes

Privileged EXEC

Examples

Example for logical chassis mode:

```
switch# show span path session 1
Session                          :1
Path                     :Te 1/0/10 -> Te 1/0/1 (ISL-exit port) -> Te 2/0/16
```

Related Commands

monitor session, source

show spanning-tree

Displays all Spanning Tree Protocol (STP) information.

Syntax

show spanning-tree [**pvst** | **mst-config** | **vlan** *vlan_id*]

Parameters

pvst
Spanning-tree PVST+ information.

mst-config
MSTP region configuration information.

vlan *vlan_id*
Specifies the VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

NOTE
Brocade Network OS supports PVST+ and Riposting. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Related Commands

show spanning-tree interface

show spanning-tree brief

Displays the status and parameters of the Spanning Tree Protocol (STP).

Syntax

show spanning-tree [**vlan** *vlan_id*] **brief**

Parameters

vlan *vlan_id*
Specifies a VLAN.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a summary of the status and parameters of STP for each interface, including the port roles and port states.

The following describes the port roles and states:

- Port roles—root port, designated port, alternate port and backup port.
- Port states—discarding, learning, forwarding, and blocked.
- Port types—edge port (PortFast), point-to-point, and shared port.

When "root guard" is in effect, the **show spanning-tree brief** command output shows the port state as ERR, not root_inc.

Examples

To display the interface summary of the Spanning Tree Protocol:

```
switch# show spanning-tree brief

Spanning-tree Mode: Rapid Spanning Tree Protocol
      Root ID      Priority 32768
                   Address  0005.1e76.1aa0
                   Hello Time 2, Max Age 20, Forward Delay 15
      Bridge ID    Priority 32768
                   Address  0005.1e76.1aa0
                   Hello Time 2, Max Age 20, Forward Delay 15, Tx-HoldCount 6
                   Migrate Time 3 sec
Interface     Role  Sts  Cost       Prio  Link-type        Boundary  Edge
--------------------------------------------------------------------------
Te 0/0        DIS   DSC  2000       128   P2P               Yes      No
Te 0/1        ALT   BLK  2000       128   P2P               Yes      No
Te 0/2        RTPT  BLK  2000       128   P2P               Yes      No
Te 0/3        DIS   BLK  2000       128   P2P               Yes      No
Te 0/8        DIS   DSC  2000       128   P2P               Yes      No
Te 0/19       DIS   DSC  2000       128   P2P               Yes      No
Te 0/20       DIS   DSC  2000       128   P2P               Yes      No
```

Typical output of a summary that contains an rbridge-id as a non-root port.

```
switch# show spanning-tree brief
Spanning-tree Mode: Rapid Spanning Tree Protocol
      Root ID      Priority 32768
                   Address  0005.1ecd.0b8a
                   Hello Time 2, Max Age 20, Forward Delay 15
      Root Port  ID : 5/0/22
      Bridge ID        Priority 32768
                       Address 0105.3352.6f27
                          STP Switch Id: 01e0.5200.0211
                       Hello Time 2, Max Age 20,
                     Forward Delay 15, Tx-HoldCount 6
                       Migrate Time 3 sec
 Interface      Role  Sts  Cost       Prio  Link-type        Edge
 ---------------------------------------------------------------------
 Te 6/0/20       DES   FWD  2000       128   P2P               No
 Te 6/0/21       DES   FWD  2000       128   P2P               No
 Te 6/0/23       ALT   DSC  2000       128   P2P               No
```

Related Commands

show spanning-tree interface

show spanning-tree interface

Displays the state of the Spanning Tree Protocol for all named port-channels or 1-gigabit Ethernet, or 10-gigabit Ethernet interfaces.

Syntax

show spanning-tree interface [**port-channel** *number* | <*N*>**gigabitethernet** *rbridge-id/slot/port*]

Parameters

port-channel *number*

Specifies the port-channel number. The number of available channels range from 1 through 6144.

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The following describes the port roles, states and types:

- Port roles—root port, designated port, alternate port and backup port.
- Port states—discarding, learning, and forwarding.
- Port types—edge port (PortFast), point-to-point, and shared port.

To display information on a 10-gigabit Ethernet interface:

```
switch# show spanning-tree interface tengigabitethernet 1/0/0
Spanning-tree Mode: Rapid Spanning Tree Protocol
 Root Id: 8000.0005.1e76.1aa0 (self)
 Bridge Id: 8000.0005.1e76.1aa0
 Port Te 0/0 enabled
     IfIndex: 67108864; Id: 8000; Role: Disabled; State: Discarding
     Designated Path Cost: 0
     Configured Path Cost: 2000
     Designated Port Id: 0; Port Priority: 128
     Designated Bridge: 0000.0000.0000.0000
     Number of forward-transitions: 0
     Version Rapid Spanning Tree Protocol - Received None - Send RSTP
     Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
        Configured Root guard: off; Operational Root guard: off
        Boundary: yes
        Bpdu-guard: off
        Bpdu-filter: off
        Link-type: point-to-point
        Received BPDUs: 0; Sent BPDUs: 0
```

Related Commands

show spanning-tree brief

show spanning-tree mst brief

Displays the status and parameters of the Multiple Spanning Tree Protocol (MSTP) instance information in brief.

Syntax

show spanning-tree mst brief

Modes

Privileged EXEC mode

Usage Guidelines

The command output includes the port roles, port states and port types.

- Port roles—root port, designated port, alternate port, and backup port.
- Port states—discarding, learning, and forwarding.
- Port types—edge port (PortFast), point-to-point, and shared port.

Examples

To display the status and parameters of the MSTP instance information:

```
switch# show spanning-tree mst brief

Spanning-tree Mode: Multiple Spanning Tree Protocol
CIST Root ID            Priority 32768
                         Address  0005.1e76.1aa0
CIST Bridge ID          Priority 32768
                         Address  0005.1e76.1aa0
CIST Regional Root ID   Priority 32768
                         Address  0005.1e76.1aa0
Configured Hello Time 2, Max Age 20, Forward Delay 15
Max Hops 20, Tx-HoldCount 6
CIST Root  Hello Time 2, Max Age 20, Forward Delay 15, Max Hops 20
CIST Root path cost 0
Interface     Role  Sts  Cost       Prio  Link-type        Boundary  Edge
-------------------------------------------------------------------------
Te 0/0        DIS   DSC  2000       128   P2P               Yes      No
Te 0/1        ALT   BLK  2000       128   P2P               Yes      No
Te 0/2        RTPT  BLK  2000       128   P2P               Yes      No
Te 0/3        DIS   BLK  2000       128   P2P               Yes      No
Te 0/8        DIS   DSC  2000       128   P2P               Yes      No
Te 0/19       DIS   DSC  2000       128   P2P               Yes      No
Te 0/20       DIS   DSC  2000       128   P2P               Yes      No
```

Related Commands

show spanning-tree mst instance, show spanning-tree mst interface

show spanning-tree mst detail

Displays details on an interface for the Multiple Spanning Tree Protocol (MSTP) instance running.

Syntax

show spanning-tree mst detail [**interface port-channel** *number* | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

interface

Specifies the interface for which to display the MSTP information.

port-channel *number*

Specifies the port-channel of the interface. The number of available channels range from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

To display MSTP information on the switch in detail:

```
switch# show spanning-tree mst detail
Spanning-tree Mode: Multiple Spanning Tree Protocol
CIST Root Id: 8000.0005.1e76.1aa0 (self)
CIST Bridge Id: 8000.0005.1e76.1aa0
CIST Reg Root Id: 8000.0005.1e76.1aa0 (self)
CIST Root Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20
Configured Forward Delay: 15; Hello Time: 2; Max Age: 20; Max-hops: 20;
Tx-HoldCount: 6
Number of topology change(s): 0
Bpdu-guard errdisable timeout: disabled
Bpdu-guard errdisable timeout interval: 300 sec
Migrate Time: 3 sec

CIST Port Details.
==================
Instance: 0; Vlans:1, 100
Port Te 0/0 enabled
    IfIndex: 67108864; Id: 8000; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0

Port Te 1/0/8 enabled
    IfIndex: 67633408; Id: 8008; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0

Port Te 1/0/19 enabled
    IfIndex: 68354563; Id: 8013; Role: Disabled; State: Discarding
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0

Port Te 1/0/20 enabled
    IfIndex: 68420100; Id: 8014; Role: Disabled; State: Discarding
```

```
    Designated External Path Cost: 0; Internal Path Cost 0
    Configured Path Cost: 2000
    Designated Port Id: 0; CIST Priority: 128
    Designated Bridge: 0000.0000.0000.0000
    CIST Port Hello Time: 2
    Number of forward-transitions: 0
    Version Multiple Spanning Tree Protocol - Received None - Send MSTP
    Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
    Configured Root guard: off; Operational Root guard: off
    Boundary: yes
    Bpdu-guard: off
    Bpdu-filter: off
    Link-type: point-to-point
    Received BPDUs: 0; Sent BPDUs: 0

MSTI details.
==============
```

Related Commands

show spanning-tree mst instance, show spanning-tree mst interface

show spanning-tree mst instance

Displays information on a specified Multiple Spanning Tree Protocol (MSTP) instance.

Syntax

show spanning-tree mst instance i *nstance_id* [**interface port-channel** *number* | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

instance_id
Specifies the MSTP instance for which to display information. Valid values range from 1 through 31.

interface
Specifies the interface for which to display the MSTP instance information.

port-channel *number*
Specifies the port-channel of the interface. The number of available channels range from 1 through 6144.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples

To display information on MSTP instance 1:

```
switch# show spanning-tree mst instance 1 interface tengigabitethernet 1/0/0

Instance: 1; VLANs: 100
MSTI Root Id: 8001.0005.1e76.1aa0 (self)
MSTI Bridge Id: 8001.0005.1e76.1aa0
MSTI Bridge Priority: 32768
```

Related Commands

show spanning-tree mst brief, show spanning-tree mst interface

show spanning-tree mst interface

Displays information for a specified interface for a Multiple Spanning Tree Protocol (MSTP) instance.

Syntax

show spanning-tree mst interface [**port-channel** *number* | *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

port-channel *number*

Specifies the port-channel of the interface. The number of available channels range from 1 through 6144.

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display MSTP protocol specific information such as Common and Internal Spanning Tree (CIST) spanning-tree related information, information to each MSTP instance (MSTI), and the state of the port specific to each MSTI.

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

To display information for the MSTP interface:

```
switch# show spanning-tree mst interface tengigabitethernet 5/0/1
Spanning-tree Mode: Multiple Spanning Tree Protocol
CIST Root Id: 8000.0005.1e76.1aa0 (self)
CIST Bridge Id: 8000.0005.1e76.1aa0
CIST Reg Root Id: 8000.0005.1e76.1aa0 (self)
IST Operational Port Hello Time: 0
Number of forward-transitions: 0
Version: Multiple Spanning Tree Protocol - Received None - Send MSTP
Edgeport: off; AutoEdge: no; AdminEdge: no; EdgeDelay: 3 sec
Configured Root guard: off; Operational Root guard: off
Boundary: yes
Bpdu-guard: off
Bpdu-filter: off
Link-type: point-to-point
Received BPDUs: 0; Sent BPDUs: 0
Instance Role   Sts   Cost   Prio VLANs
------------------------------------------------------------------------
0                           DIS       DSC   2000       128             1
```

Related Commands

show spanning-tree brief, show spanning-tree mst brief

show ssh server status

Displays the current Secure Shell (SSH) server key-exchange status.

Syntax

show ssh server status [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Speccifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

When SSH server is disabled in rbridge-id 3:

```
switch# show ssh server status rbridge-id 3
rbridge-id 3 SSH server status: Enabled
switch#
```

When SSH server key-exchange method is configured to DH Group 14:

```
switch# show ssh server status rbridge-id 3
rbridge-id 3
SSH Kex Exchange Algorithm: DH Group 14
```

When SSH Server Key-exchange method is restored to default

```
switch# show ssh server status rbridge-id 3
rbridge-id 3
```

Related Commands

show telnet server status, ssh, ssh server shutdown

show ssh server rekey-interval status

Displays the status information related to the Secure Shell (SSH) server rekey-interval.

Syntax

show ssh server rekey-interval status

Modes

Privileged EXEC mode

show startup-config

Displays the contents of the startup configuration.

Syntax

show startup-config

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

To display the startup configuration:

```
switch# show startup-config

chassis virtual-ip 10.24.73.50/20
no diag post enable
linecard 2 LC48x10G
linecard 4 LC48x10G
class-map default
match any
!
logging rbridge-id 1
raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
switch-attributes 1
chassis-name VDX8770-4
host-name sw0
!
support rbridge-id 1
ffdc
!
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common!
(Output truncated)
```

Related Commands

show running-config, show startup-db

show startup-db

Displays the startup database information.

Syntax

show startup-db

Parameters

Refer to the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **show startup-db ?** to display the list of available database entries.

Examples

To display the logging configuration in the startup database:

```
switch# show startup-db logging

logging rbridge-id 1
 raslog console INFO
!
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
```

Related Commands

show running-config, show startup-config

show statistics access-list

For a given network protocol and inbound/outbound direction, displays ACL statistical information. You can show statistics for a specified ACL or only for that ACL on a specified interface. You can also display statistical information for all ACLs bound to a specified switch interface, VLAN, VE, or VXLAN overlay gateway.

Syntax

The following version displays statistical information for either the inbound or the outbound direction of a specified ACL:
show statistics access-list { **ip** | **ipv6** | **mac** } *name* { **in** | **out** }

For either the inbound or the outbound direction on a specified N-gigabite physical Ethernet, port-channel, or VLAN interface, the following version displays statistical information for all ACLs bound to that interface:
show statistics access-list interface { *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

For either the inbound or the outbound direction on a specified virtual Ethernet (VE) interface, the following version displays statistical information for all ACLs bound to that interface. You can also include ACLs specific to an RBridge:
show statistics access-list interface ve *vlan_id* { **in** | **out** } [**rbridge-id** { *rbridge_id* | **all** }]

For the inbound direction on a specified VXLAN overlay-gateway, the following version displays statistical information for all ACLs bound to that gateway:
show statistics access-list overlay-gateway *overlay_gateway_name* **in**

For either the inbound or the outbound direction, on a specified N-gigabite physical Ethernet, port-channel, or VLAN interface, the following version displays statistics of the rules in a specified MAC ACL bound to that interface:
show statistics access-list mac *name* **interface** { *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

For either the inbound or the outbound direction, on a specified N-gigabite physical Ethernet or port-channel interface, the following version displays statistics of the rules in a specified Layer 3 ACL bound to that interface:
show statistics access-list { **ip** | **ipv6** } *name* **interface** { *<N>***gigabitethernet** *rbridge_id/slot/port* | **port-channel** *index* } { **in** | **out** }

For either the inbound or the outbound direction, on a specified virtual Ethernet (VE) interface, the following version displays statistics of the rules in a specified Layer 3 ACL bound to that interface. You can also include ACLs specific to an RBridge:
show statistics access-list { **ip** | **ipv6** } *name* **interface ve** *vlan_id* **in** | **out** } [**rbridge-id** { *rbridge_id* | **all** }]

Parameters

ip | **ipv6** | **mac**
: Specifies the network protocol.

name
: Specifies the ACL name.

interface
: Filter by interface.

*<N>***gigabitethernet**
: Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge_id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel. Available channels range from 1 through 6144.

vlan *vlan_id*
(Available only on Layer 2) Specifies a VLAN.

ve *vlan_id*
(Available only on Layer 3) Specifies a virtual Ethernet (VE).

rbridge-id
(for a VE interface) To display ACLs beyond the local node, include this keyword and the relevant of the following:

rbridge-id
Specifies an RBridge ID.

all
Specifies all RBridges.

overlay-gateway *overlay_gateway_name*
Specifies a VXLAN overlay-gateway.

in | **out**
Specifies the ACL binding direction (incoming or outgoing).

Modes

Privileged EXEC mode

Usage Guidelines

Statistics are displayed only for rules that contain the **count** keyword.

Command Output

The **show statistics access-list** command displays the following information:

Output field	Description
Uncount	The counter resource is not allocated. This is typically seen if counting is not supported or if the hardware resources limit is reached.
Unwritten	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays inbound ACL statistics for a named IPv4 ACL:

```
switch# show statistics access-list ip l3ext in
ip access-list l3ext TenGigabitEthernet 1/1/8 in
seq 76 deny ip 10.10.75.10 0.0.0.0 any count log (795239 frames)
seq 77 hard-drop ip 10.10.75.10 0.0.0.0 10.10.11.0 0.0.0.255 count log (0 frames)
seq 78 hard-drop ip any 10.10.11.0 0.0.0.255 count log (0 frames)
seq 79 hard-drop ip any 10.10.0.0 0.0.255.255 count log (0 frames)
seq 80 hard-drop ip 10.10.75.10 0.0.0.0 any count log (0 frames)
seq 81 hard-drop ip 10.10.75.0 0.0.0.0 10.10.0.0 0.0.255.255 count log (0 frames)
seq 91 hard-drop ip any any count (0 frames)
seq 100 deny udp 10.10.75.0 0.0.0.255 10.10.76.0 0.0.0.255 count log (0 frames)
seq 1000 permit ip any any count log (0 frames)
```

The following example displays inbound ACL statistics for a specified ten-gigabite interface:

```
switch# show statistics access-list interface tengigabitethernet 1/4/1 in
ipv6 access-list ipv6-std-acl on TenGigabitEthernet 1/4/1 at Ingress (From User)
    seq 10 permit host 0:1::1
    seq 20 deny 0:2::/64
    seq 30 hard-drop any count (100 frames)
```

The following example displays inbound statistics for all ACLs bound to a specified VE interface:

```
switch# show statistics access-list interface ve 3010 in
ipv6 access-list ip_acl_3 on Ve 3010 at Ingress (From User)
    seq 10 deny ipv6 2001:3010:131:35::/64 2001:1001:1234:1::/64 count (0 frames)
    seq 20 permit ipv6 2001:3010:131:35::/64 2001:3001:1234:1::/64
```

The following example displays (inbound) statistics for all ACLs bound to an overlay gateway:

```
switch# show statistics access-list overlay-gateway gw121 in
mac access-list stdmacaclin on overlay-gateway gw121 at Ingress (From User)
ip access-list stdipaclin on overlay-gateway gw121 at Ingress (From User)
ipv6 access-list stdipv6aclin on overlay-gateway gw121 at Ingress (From User)
```

Related Commands

access-group, access-list, clear counters access-list, show access-list, show running-config access-list

show storm-control

Displays information for traffic controlled by configured rate limits.

Syntax

show storm-control

show storm-control broadcast [**interface** { *<N>***gigabitethernet** } *rbridge-id/slot/port*]

show storm-control multicast [**interface** { *<N>***gigabitethernet** } *rbridge-id/slot/port*]

show storm-control unknown-unicast [**interface** { *<N>***gigabitethernet** } *rbridge-id/slot/port*]

Parameters

storm-control
Displays all BUM (Broadcast, Unknown unicast and Multicast)-related configurations in the system.

broadcast
Displays all BUM-related configurations in the system for the broadcast traffic type.

interface
Displays all BUM-related configurations in the system for the specified interface.

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

multicast
Displays all BUM-related configurations in the system for the multicast traffic type.

unknown-unicast
Displays all BUM-related configurations in the system for the unknown-unicast traffic type.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display BUM storm-control-related configuration for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interface.

Examples

To display storm-control information for broadcast traffic on the 10-gigabit Ethernet interface 102/4/1:

```
switch# show storm-control broadcast interface tengigabitethernet 102/4/1

Interface   Type          rate (Mbps)  conformed    violated      total
Te102/4/1   broadcast     100,000      12500000000  12500000000   25000000000
```

To display storm-control information for all traffic on the 10-gigabit Ethernet interface 102/4/1:

```
switch# show storm-control interface tengigabitethernet 102/4/1

Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/1   unknown-unicast  100,000      12500000000 12500000000 25000000000
Te102/4/1   multicast        100,000      12500000000 12500000000 25000000000
```

To display storm-control information for all traffic in the system:

```
switch# show storm-control

Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/1   unknown-unicast  100,000      12500000000 12500000000 25000000000
Te102/4/1   multicast        100,000      12500000000 12500000000 25000000000
Te102/4/2   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/3   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/4   unknown-unicast  100,000      12500000000 12500000000 25000000000
```

To display storm-control information for all broadcast traffic the system:

```
switch# show storm-control broadcast

Interface   Type             rate (Mbps)  conformed   violated    total
Te102/4/1   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/2   broadcast        100,000      12500000000 12500000000 25000000000
Te102/4/3   broadcast        100,000      12500000000 12500000000 25000000000
```

show support

Displays a list of core files on the switch.

Syntax

show support [**rbridge-id** { *rbridge-id* | **all** }]

Command Default

Displays information for the local switch.

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all switches in the fabric.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Pagination is not supported with this command. Use the "more" parameter to display the output one page at a time.

Examples

To display the core files:

```
switch# show support

No core or FFDC data files found!
```

Related Commands

clear support, copy support, show running-config support

show system

Displays hardware and software system information.

Syntax

show system { **rbridge-id** *rbridge-id* }

Parameters

rbridge-id *rbridge-id*
Specifies an RBridge ID.

Modes

Privileged EXEC mode

Examples

To display the system information:

```
switch# show system

Stack MAC                     : 00:05:33:4B:CC:37
  -- UNIT 0 --
Unit Name                     : sw0
Switch Status                 : Online
Hardware Rev                  : 97.4
Ten Gigabit Ethernet Port(s)  : 60
Up Time                       : up 1 day, 2:29
Current Time                  : 21:20:50 GMT
NOS Version                   :
Jumbo Capable                 : yes
Burned In MAC                 : 00:05:33:4B:CC:37
Management IP                 : 10.24.85.74
Management Port Status        : UP
  -- Power Supplies --
PS1 is faulty
PS2 is OK
  -- Fan Status --
Fan 1 is Ok
Fan 2 is Ok
Fan 3 is Ok
```

Related Commands

show version

show system internal nas

Displays all NAS server IP addresses in the system.

Syntax

show system internal nas

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Examples

To display the IP addresses for all active NAS servers:

```
switch0# show system internal nas
Rbridge 1
-----------
Auto-NAS Enabled
Cos 2
Dscp 10
Traffic Class 5
nas server-ip 10.192.100.100/32 vlan 100
nas server-ip 10.192.100.101/32 vrf brown
```

Related Commands

backup-advertisement-interval, clear nas statistics, nas auto-qos, nas server-ip, show cee maps, show nas statistics, show running-config nas server-ip, show system internal nas

show system monitor

Displays the overall status for a selected switch.

Syntax

show system monitor { **rbridge-id** [*rbridge-id* | **all**] }

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to display the overall switch status and the status of the contributors defined as part of the policy.

This command is supported only on the local switch.

Examples

```
switch# show system monitor

** System Monitor Switch Health Report **
RBridge 128     switch status            : HEALTHY
                Time of Report           : 2012-06-19 03:18:28
                Power supplies monitor   : HEALTHY
                Temperatures monitor     : HEALTHY
                Fans monitor             : HEALTHY
                CID-Card monitor         : HEALTHY
                MM monitor               : HEALTHY
                LC monitor               : HEALTHY
                SFM monitor              : HEALTHY
                Flash monitor            : HEALTHY
```

Related Commands

system-monitor, system-monitor-mail

show telnet server status

Displays the current Telnet server status.

Syntax

show telnet server status [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Examples

When Telnet server status is enabled:

```
switch# show telnet server status [rbridge-id
rbridge-id
 | all]
Telnet server status: Enabled
```

When Telnet server is disabled in rbridge-id 3:

```
switch# show telnet server status rbridge-id 3
rbridge-id 3 Telnet server status: Disabled
switch#
```

Related Commands

show running-config telnet server, telnet server shutdown

show threshold monitor

Displays the current status of environmental thresholds and alerts for interfaces, security, and SFPs.

Syntax

show threshold monitor [**interface all area** | **security area** [**login-violation** [**rbridge-id** *rbridge-id* | *all*] | **telnet-violation** [**rbridge-id** *rbridge-id* | *all*]] | **sfp all area** [**current** | **rxp** | **temperature** | **txp** | **voltage**]

Parameters

interface all area
Displays status of interface thresholds and alerts.

security area
Displays status of security thresholds and alerts.

login-violation
Displays status of login violations.

telnet-violation
Displays status of Telnet violations.

sfp all area
Displays status of SFP thresholds and alerts.

current
Amount of current supplied to the SFP transceiver.

rxp
Amount of incoming laser power, in microWatts (µW).

temperature
Temperature of the SFP, in degrees Celsius.

txp
Amount of outgoing laser power, in microWatts (µW).

voltage
Amount of voltage supplied to the SFP.

rbridge-id *rbridge-id*
Specifies a switch by means of the switch's RBridge ID.

all
Reports status for all nodes in the cluster.

Modes

Privileged EXEC mode

Examples

```
switch# show threshold monitor security area login-violation rbridge-id all
Rbridge-Id    Area                          Value   Status     Monitoring Status
154           Login Violation               0       In Range   Monitoring
```

Related Commands

show defaults threshold, system-monitor, system-monitor-mail, threshold-monitor interface

show tunnel

Displays statistics for tunnels.

Syntax

show tunnel *ID* [**rbridge-id** *rbridge-id*]

show tunnel [**site** *name*] **brief** [**rbridge-id** *rbridge-id*]

show tunnel dst-ip *dst_ip_address* **brief** [**rbridge-id** *rbridge-id*]

show tunnel mode vxlan brief [**rbridge-id** *rbridge-id*]

show tunnel nsx service-node [**rbridge-id** *rbridge-id*]

show tunnel overlay-gateway *name* **brief** [**rbridge-id** *rbridge-id*]

show tunnel src-ip *src_ip_address* **brief** [**rbridge-id** *rbridge-id*]

show tunnel statistics [**rbridge-id** *rbridge-id*]

Parameters

tunnel *ID*
Specifies one tunnel ID for which to show statistics. Range is 1 to 65535.

rbridge-id *rbridge-id*
Specifies an RBridge ID.

site *name*
Specifies a site that represents a remote VCS Fabric or the other end of the tunnel.

brief
Displays brief listings for all tunnels.

dst-ip *dst_ip_address*
Filters statistics by tunnel destination IP address.

mode
Filters statistics by tunnel mode; in Network OS, the only supported mode is vxlan.

vxlan
Filters statistics on all VXLANs.

nsx service-node
Filters BUM-enabled tunnels to NSX service nodes.

overlay-gateway *name*
Filter by gateway name.

src-ip *src_ip_address*
Filters statistics by tunnel source IP address.

statistics
Displays packet information for all tunnels.

Modes

Privileged EXEC mode

Usage Guidelines

This command lists statistics for all the tunnels in the VCS. The output includes the tunnel ID, source IP address, destination IP address, VRF, administration state, and operational state.

For **show tunnel** *ID*, details of the specified tunnel are shown. Output includes the tunnel ID, tunnel IF index, administration state, operational state, source IP address, gateway (if any), destination IP address, packet count, byte count, and current outgoing path.

For **show tunnel statistics**, you receive packet information for all tunnels.

This command is available only for a switch that is in logical chassis cluster mode.

To show brief listings for all tunnels in the VCS:

```
switch# show tunnel brief
Tunnel 1, mode VXLAN
Admin state: Up, Oper state: Up
Source IP 10.10.10.1, Vrf default
Destination IP 150.1.1.1

Tunnel 200, mode VXLAN
Admin state: Up, Oper state: Down
Source IP 100.1.1.11, Vrf default
Destination IP 160.1.1.1

Tunnel 300, mode VXLAN
Admin state: Up, Oper state: Up
Source IP 100.1.1.11, Vrf default
Destination IP 170.1.1.1
```

To display statistics for a tunnel site:

```
switch# show tunnel site VCS_2 brief
Tunnel 61441, mode VXLAN, rbridge-ids 10
Admin state UP, Oper state UP
Source IP 10.2.2.1, Vrf default-vrf
Destination IP 10.1.1.1
```

To display statistics for VLANs attached to the overlay gateway:

To show statistics for the tunnel with the ID of 100:

```
switch# show tunnel 61441
  Tunnel 61441, mode VXLAN, rbridge-ids 1,4
  Ifindex 1000000, Admin state up, Oper state down
  Overlay gateway "myGateway", ID 1
  Source IP 10.10.10.1 ( Loopback 10 ), Vrf blue
  Destination IP 60.60.60.1, Site mySite1
  Active next hop on rbridge 1: (none)
  Active next hop on rbridge 4: (none)
  Packet count: RX 0               TX 0
  Byte count  : RX (NA)            TX 0
```

To show high-level statistics for all tunnels:

```
switch# show tunnel statistics

Tunnel     Packets        Bytes
ID        TX     RX       TX          RX
-------------------------------------------------------
1         22200  2272     1982888     11000
200       2233   888922   22333       7867822
```

show udld

Shows global UDLD information.

Syntax

show udld

Modes

Privileged EXEC mode

Usage Guidelines

This command displays global unidirectional link detection (UDLD) protocol configuration values such as whether the protocol is enabled on the switch and the *hello* time and timeout values.

Examples

To display global UDLD information on the switch:

```
switch# show udld
UDLD Global Information
  Admin State:       UDLD enabled
  UDLD hello time:   500 milliseconds
  UDLD timeout:      2500 milliseconds
```

Related Commands

protocol udld

show udld interface

Dis[plays unidirectional link detection (UDLD) protocol information for the specified interfaces.

Syntax

show udld interface [*<N>***gigabitethernet** *rbridge-id/slot/port* }]

Parameters

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The following describes the values that appear in the headings for this command.

TABLE 17 Description UDLD headings

Heading	Description
State	Describes if UDLD is enable or disabled.
Mode	Describes if the mode is Receive, Transmit, or Both (Transmit/ Receive).
Advertise Transmitted	Describes how often the advertisement is transmitted.
Hold time for advertise	Describes the hold time for receiving devices before discarding.
Re-init Delay Timer	The timer for the reinitializing delay
Tx Delay Timer	The timer for transmission
DCBX Version	The current DCBX version
Auto-Sense	States whether Auto-Sense is active.
Transmit TLVs	Describes what information is being transmitted for the TLV.
DCBX FCoE Priority Bits	Describes the current FCoE priority bit for DCBX.

Examples

To display UDLD information for a specific 10-gigabitEthernet interface:

```
switch# show udld interface te 5/0/1
Global Admin State:  UDLD enabled
UDLD information for TenGigabitEthernet 5/0/1
  UDLD Admin State:                  Enabled
  Interface Operational State:       Link is down
  Remote hello time:                 Unknown
  Local system id:  0x1ecd7bfa       Remote system id: Unknown
  Local port :      5/0/1            Remote port :     Unknown
  Local link id:    0x0              Remote link id:   Unknown
  Last Xmt Seq Num: 1                Last Rcv Seq Num: Unknown
```

Related Commands

protocol udld

show udld statistics

Shows UDLD statistics.

Syntax

show udld statistics [**interface** { <*N*>**gigabitethernet** *rbridge-id/slot/port* }]

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays all unidirectional link detection (UDLD) protocol statistics or shows the statistics on a specified por

Examples

To show UDLD statistics on a specific 10-gigabitEthernet interface:

```
switch# show udld statistics interface te 5/0/1
```

Related Commands

protocol udld

show users

Displays the users logged in to the system and locked user accounts.

Syntax

show users [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

RBridge ID mode

Examples

To display active user sessions and locked user accounts:

```
switch# show users
 rbridge-id
 all
**USER SESSIONS**
RBridge ID      Username  Role   Device  Time Logged In
195             admin     admin  Cli     2014-01-15 15:11:26
**LOCKED USERS**
RBridge ID      Username
no locked users
```

Related Commands

show running-config username

show vcs

Displays the Brocade VCS Fabric configuration.

Syntax

show vcs { **detail** | **virtual-ip** }

Parameters

detail

Displays detailed information about each RBridge in the fabric.

virtual-ip

Displays the virtual IP address.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the Brocade VCS Fabric parameters (VCS ID and the switch RBridge ID) and Brocade VCS Fabric mode.

Examples

To display the VCS summary view for a switch that is in fabric cluster mode ("Local-Only"):

```
switch# show vcs

Config Mode    : Local-Only
VCS ID         : 1
Total Number of Nodes           : 1
Rbridge-Id  WWN                       Management IP   VCS Status  Fabric Status        HostName
1           10:00:00:05:33:51:63:42* 10.17.37.154    Online      Online               sw0
```

To display the VCS configuration details:

```
switch# show vcs detail

Config Mode    : Local-Only
VCS ID         : 1
Total Number of Nodes           : 6
Node :1
    Serial Number : BKN2501G00R
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 38
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:52:2A:82
    Switch MAC    : 00:05:33:52:2A:82
    FCF MAC       : 0B:20:B0:64:10:27
    Switch Type   : BR-VDX6720-24-C-24
    Internal IP   : 127.1.0.38
    Management IP : 10.17.10.38
Node :2
    Serial Number : BZA0330G00P
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 80*
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:78:00:00
    Switch MAC    : 00:05:33:78:00:81
    FCF MAC       : 19:30:00:48:19:31
    Switch Type   : Brocade VDX 8770-4
    Internal IP   : 127.1.0.80
    Management IP : 10.17.11.80
Node :3
    Serial Number : BWW2516G01G
    Condition     : Good
    Status        : Connected to Cluster
    VCS Id        : 1
    Rbridge-Id    : 82
    Co-ordinator  : NO
    WWN           : 10:00:00:05:33:6F:2B:D2
    Switch MAC    : 00:05:33:6F:2B:D2
    FCF MAC       : 0B:20:B0:64:10:26
    Switch Type   : Elara2f
    Internal IP   : 127.1.0.82
    Management IP : 10.17.10.82
(Output truncated)
```

To display the VCS summary view for a switch (called *rb1)* that is in logical chassis cluster mode ("Distributed"):

```
rb1# show vcs
Config Mode    : Distributed
VCS ID         : 300
VCS GUID       : 1001bffd-24f5-4a11-8adf-d00991dcae48
Total Number of Nodes           : 3
Rbridge-Id       WWN                                       Management IP
Status                              HostName
-------------------------------------------------------------------------------
1                       10:00:00:05:1E:CD:22:6A*   10.17.10.21        Online       rb1
2                 >10:00:00:05:1E:CD:11:6A   10.17.10.22        Online       rb2
3                 10:00:00:05:33:00:6C:80    10.17.10.23        Online       sw0
```

To display the VCS configuration details:

```
rb1# show vcs detail
Config Mode    : Distributed
VCS ID         : 300
VCS GUID       : 1001bffd-24f5-4a11-8adf-d00991dcae48
Total Number of Nodes           : 3
Nodes Disconnected from Cluster : 0
Cluster Condition               : Good
Cluster Status                  : All Nodes Present in the Cluster
Node :1
    Serial Number      : BKH0322F01L
    Condition          : Good
    Status             : Connected to Cluster
    VCS Id             : 300
    Rbridge-Id         : 1*
    Co-ordinator       : NO
    WWN                : 10:00:00:05:1E:CD:22:6A
    Switch MAC         : 00:05:1E:CD:22:6A
    FCF MAC            : 00:05:1E:CD:22:6A
    Switch Type        : VDX6720-24
    Firmware Ver       : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
    Internal IP        : 127.1.0.1
    Management IP      : 10.17.10.21
Node :2
    Serial Number      : BKH0322F01Y
    Condition          : Good
    Status             : Co-ordinator
    VCS Id             : 300
    Rbridge-Id         : 2
    Co-ordinator       : YES
    WWN                : 10:00:00:05:1E:CD:11:6A
    Switch MAC         : 00:05:1E:CD:11:6A
    FCF MAC            : 00:05:1E:CD:11:6A
    Switch Type        : VDX6720-24
    Firmware Ver       : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
    Internal IP        : 127.1.0.2
    Management IP      : 10.17.10.22
Node :3
    Serial Number      : BKH0320F005
    Condition          : Good
    Status             : Connected to Cluster
    VCS Id             : 300
    Rbridge-Id         : 3
    Co-ordinator       : NO
    WWN                : 10:00:00:05:33:00:6C:80
    Switch MAC         : 00:05:33:00:6C:80
    FCF MAC            : 00:05:33:00:6C:80
    Switch Type        : VDX6720-24
    Firmware Ver       : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
    Internal IP        : 127.1.0.3
    Management IP      : 10.17.10.23
```

To issue the **show vcs** command on a VCS-disabled switch:

```
switch# show vcs

state      : Disabled
```

To display the virtual IP address:

```
switch# show vcs virtual-ip

Virtual IP                     : 10.21.87.2/20
Associated rbridge-id         : 2
```

show version

Displays the current firmware version.

Syntax

show version [**rbridge-id** { *rbridge-id* | **all** }] [**all-partitions**] [**brief**]

Parameters

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

all-partitions

Displays firmware information for both the active and the standby partitions. For each module, both partitions are displayed.

brief

Displays a brief version of the firmware information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display firmware version information and build dates. The default command output includes the following information:

- Network Operating System Version—The firmware version number
- Firmware name—The label of the firmware image
- Build Time—The build date and time of the firmware
- Install time—The date and time of the firmware installation
- Kernel—The Linux kernel version
- Boot-Prom—The size of the boot programmable read-only memory
- Control Processor—The control processor model and memory

When executed on the active management module, this command displays firmware versions on both management modules and interface modules. When executed on the standby management module, only the firmware versions for the standby management module are displayed.

The **rbridge-id** and **all** operands are not supported.

Examples

To display the firmware version information for all partitions:

```
switch# show version all-partitions

Network Operating System Software
Network Operating System Version: 3.0.0
Copyright (c) 1995-2012 Brocade Communications Systems, Inc.
Firmware name:      3.0.0
Build Time:         01:18:17 May 26, 2012
Install Time:       10:16:24 May 27, 2012
Kernel:             2.6.34.6
BootProm:           1.0.0
Control Processor:  e500mc with 7168 MB of memory
Slot    Name    Primary/Secondary Versions      Status
-----------------------------------------------------
 M1     NOS     4.1.0                           STANDBY
                4.1.0
 M2     NOS     4.1.0                           ACTIVE*
                4.1.0
 L1/0   NOS     4.1.0                           ACTIVE
                4.1.0
 L1/1   NOS     4.1.0                           STANDBY
                4.1.0
 L2/0   NOS     4.1.0                           ACTIVE
                4.1.0
 L2/1   NOS     4.1.0                           STANDBY
                4.1.0
```

To display the firmware for all partitions in the brief view:

```
switch# show version all-partitions brief

Slot    Name    Primary/Secondary Versions      Status
-----------------------------------------------------
 M1     NOS     4.1.0                           STANDBY
                4.1.0
 M2     NOS     4.1.0                           ACTIVE*
                4.1.0
 L1/0   NOS     4.1.0                           ACTIVE
                4.1.0
 L1/1   NOS     4.1.0                           STANDBY
                4.1.0
 L2/0   NOS     4.1.0                           ACTIVE
                4.1.0
 L2/1   NOS     4.1.0                           STANDBY
                4.1.0
```

Related Commands

firmware download, show firmwaredownloadstatus

show virtual-fabric status

Displays the status of the Virtual Fabric (VF): VF-capable, VF-incapable, or VF-enabled.

Syntax

show virtual-fabric status

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the status of the VF with respect to all nodes in the fabric. The possible states are as follows:

- VF-capable: All nodes in the fabric can support service or transport VFs.
- VF-incapable: At least one node in the fabric cannot support service or transport VFs.
- VF-enabled: The Virtual Fabric is already enabled and service or transport VFs are supported

Examples

```
Typical command output display.
switch# show virtual-fabric status
Fabric is virtual-fabric incapable
Rbridge-Id     Virtual-fabric status
================================
1              capable
2              capable
3              incapable
4              capable
```

show vlan

Displays information about one or more VLAN interfaces.

Syntax

show vlan [*vlan_id* | **brief** [**provisioned** | **unprovisioned**] | **classifier**]

Parameters

vlan_id
: Specifies the VLAN interface to display.

brief
: Displays VLAN information for all interfaces including static and dynamic.

classifier
: Displays all VLAN classification information.

provisioned
: Displays provisioned VLANs.

unprovisioned
: Displays unprovisioned VLANs.

Modes

Privileged EXEC mode

Examples

The following example displays information about an 802.1Q VLAN:

```
switch# show vlan 1

VLAN     Name            State   Ports
                                 (u)-Untagged, (t)-Tagged
                                 (c)-Converged
======= ================ ======= ================================
1       default          ACTIVE  Te 0/0(t)
                                 Te 0/8(t)
                                 Po 1(t)
```

The following example shows all VLANs that are configured, provisioned (active) and unprovisioned (inactive):

```
switch# show vlan brief

Total Number of VLANs configured:    6
Total Number of VLANs unprovisioned: 0
Total Number of VLANs provisioned:   6
VLAN        Name         State   Ports             Classification
(F)-FCoE                         (u)-Untagged,
(T)-Transparent                  (t)-Tagged
(R)-RSPAN                        (c)-Converged
 ========================================
300         vlan300      ACTIVE      Te 4/0/1(t)
5000(T)     vlan5000     ACTIVE      Te 2/0/1/(t)  ctag 50, 60, 100-200
                                     Te 4/0/1(t)   ctag 50, 60, 100-200
5500(T)     vlan5500     ACTIVE      Te 3/0/1/(t)  ctag 1, 1002, 4093, 4095
5800        vlan5800     ACTIVE      Te 2/0/1(t)   ctag 800
6000(T)     vlan6000     ACTIVE      Te 4/0/1/(t))
```

The following example shows only provisioned VLANs:

```
switch# show vlan brief provisioned
Total Number of VLANs configured:    8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:   5
VLAN        Name         State   Ports             Classification
(F)-FCoE                         (u)-Untagged,
                                 (t)-Tagged
(R)-RSPAN                        (c)-Converged
 ========================================
1           default      ACTIVE  Te 2/0/5(c)
5000        VLAN5000     ACTIVE  Te 2/0/5(t)       ctag 100
                                 Te 2/0/6(u)       ctag 200
                                 Te 3/0/4(u)
                                 Te 3/0/5(u)       mac 0004.0004.0004
6000        VLAN6000     ACTIVE  Te 2/0/5(t)       ctag 300
                                 Te 3/0/5(u)       mac 0002.0002.0002
                                 Te 3/0/5 (u)      mac-group 1
                                 Po 10(t)          ctag 300
7000        VLAN7000     ACTIVE  Te 2/0/5 (t)      ctag 400
                                 Te 3/0/5 (u)      mac 0006.0006.0006
                                 Te 3/0/5 (u)      mac-group 2
1002(F)     VLAN1002     ACTIVE  Te 2/0/16(t)
                                 Te 3/0/15(t)
```

The following example shows only unprovisioned VLANs:

```
switch# show vlan brief unprovisioned
Total Number of VLANs configured:      8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:     5
VLAN             Name          State                  Ports
(F)-FCoE                                        (u)-Untagged, (t)-Tagged
(R)-RSPAN                                                      (c)-Converged
======== ================ ======= ======
2000           VLAN2000      INACTIVE(unprovisioned)
4000           VLAN4000      INACTIVE(unprovisioned)
8000           VLAN8000      INACTIVE(unprovisioned)
```

show vlan brief

Displays basic information about switch VLAN interfaces. You can filter to display only provisioned or unprovisioned VLANs.

Syntax

show vlan brief [**provisioned** | **unprovisioned**]

Parameters

provisioned
Displays provisioned VLANs.

unprovisioned
Displays unprovisioned VLANs.

Modes

Privileged EXEC mode

Command Output

The **show vlan brief** command displays the following information:

Output field	Description
VLAN	Displays the *vlan_ID*.
Name	Displays one of the following strings: • "default" • A name assigned to the VLAN using the **name** command • A default name automatically assigned to the VLAN, composed of "VLAN" and the *vlan_ID*. For example, if the *vlan_ID* is 1000, the default name is VLAN1000.
State	Displays "ACTIVE" for provisioned VLANs or "INACTIVE" for unprovisioned VLANs.
Ports	Displays the ports on which the VLAN is applied.
Classification	(Available only for provisioned).

Examples

The following example shows all VLANs that are configured, provisioned (active) and unprovisioned (inactive). VLAN 5800 was assigned the name "marketing."

```
switch# show vlan brief

Total Number of VLANs configured:    6
Total Number of VLANs unprovisioned: 0
Total Number of VLANs provisioned:   6
VLAN        Name         State   Ports             Classification
(F)-FCoE                         (u)-Untagged,
(T)-Transparent                  (t)-Tagged
(R)-RSPAN                        (c)-Converged
 ========================================
300         vlan300      ACTIVE      Te 4/0/1(t)
5000(T)     vlan5000     ACTIVE      Te 2/0/1/(t)  ctag 50, 60, 100-200
                                     Te 4/0/1(t)   ctag 50, 60, 100-200
5500(T)     vlan5500     ACTIVE      Te 3/0/1/(t)  ctag 1, 1002, 4093, 4095
5800        marketing    ACTIVE      Te 2/0/1(t)   ctag 800
6000(T)     vlan6000     ACTIVE      Te 4/0/1/(t))
```

Related Commands

name (VLAN interfaces)

show vlan classifier

Displays information about a specific VLAN classifier group.

Syntax

show vlan classifier [**group** *number* | **interface** *group-number* | **interface port-channel** *number* | **rule** *number* | **interface** *<N>***gigabitethernet** *rbridge-id/slot/port*]

Parameters

group *number*

Specifies the VLAN classifier group number. Valid values range from 1 through 16.

interface *group number*

Specifies the VLAN classifier interface group number. Valid values range from 1 through 16.

interface port-channel *number*

Specifies the VLAN classifier port-channel number. Valid values range from 1 through 63.

rule *number*

Specifies the VLAN classifier rule number. Valid values range from 1 through 256.

interface *<N>***gigabitethernet**

Specifies a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about all configured VLAN classifier groups or a specific VLAN interface group.

If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

show vlan private-vlan

Displays information about private VLANs.

Syntax

show vlan private-vlan

Modes

Privileged EXEC mode

Examples

```
Typical command output display.
switch# show vlan private-vlan

Primary   Secondary Type      Ports          Classification
=======   =======   ======    ===========    ==============================
6000                primary   Te 4/1/17(t)                    ctag 10
                              Te 1/2/17(t)                    ctag 10
6000      6001      isolated  Te 4/1/17(t)                    ctag 11
                              Te 2/0/17(t)                    ctag 11
6000      6002      community Te 4/1/17(t)                    ctag 12
                              Te 3/1/17(t)                    ctag 12
6000      6003      community Te 4/1/17(t)                    ctag 13
                              Te 3/1/18(t)                    ctag 13
```

show vlan rspan-vlan

Displays information about remote SPAN VLANs.

Syntax

show vlan rspan-vlan

Modes

Privileged EXEC mode

Examples

```
sw0(conf-if-te-1/1/34)# do show vlan rspan-vlan
Total Number of VLANs configured    : 3
Total Number of VLANs provisioned   : 2
Total Number of VLANs unprovisioned : 1
VLAN          Name        State                      Ports        Classification
============= =========== ======================     ============ ======
6000(R)       VLAN6000    INACTIVE(member port down) Te 1/1/34(t) ctag 121
6001(R)       VLAN6001    INACTIVE(member port down) Te 1/1/34(t) ctag 555
```

Related Commands

rspan-vlan

show vnetwork

Displays virtual assets from the vCenter that are discovered on a Brocade VDX switch.

Syntax

show vnetwork [**datacenter** [*datacenter_id* | **vcenter** *vcenter_name*] | [**diff datacenter** datacenter_id] | **dvpgs** [**datacenter** *datacenter_id* | **name** *string*] { **vcenter** *vcenter_name* } | **dvs** [**datacenter** *datacenter_id* | **name** *string*] { **vcenter** *vcenter_name* } | **hosts** [**datacenter** *datacenter_id* | **name** *string*] { **vcenter** *vcenter_name* } | **pgs** [**datacenter** *datacenter_id* | **name** *string*] { **vcenter** *vcenter_name* } | **vcenter status** | **vmpolicy** [**macaddr** [**datacenter** *datacenter_id* | **mac** *mac_address*] { **vcenter** *string* } | **vms** | **vss** [**datacenter** *datacenter_id* | **name** *string*] { **vcenter** *vcenter_name* }]

Parameters

datacenter

Displays discovered data centers.

datacenter_id

Datacenter ID (a string).

vcenter*vcenter_name*

Specifies a vCenter.

diff

Displays configuration differences between the current device and the specified data center. Refer to the **vnetwork reconcile vcenter** command for corrections.

datacenter

Specifies a data center.

datacenter_id

Datacenter ID (a string).

dvpgs

Displays distributed virtual port groups.

datacenter *datacenter_id*

Specifies a datacenter. This is optional and need not be used unless required.

name *string*

Specifies a distributed virtual port group.

dvs

Displays distributed virtual switches.

name *string*

Selects a distributed virtual switch name. This is optional and need not be used unless required.

hosts

Displays discovered hosts.

name *string*

Specifies a host name.

vcenter *vcenter_name*
Specifies a vCenter (required).

pgs
Displays discovered standard port groups.

name *string*
Specifies a standard port group.

vcenter status
Displays configured vCenter status.

vmpolicy
Displays association between virtual network interface cards (vNICs) or VM kernel NICs (vmkNICs) and port groups or port profiles.

macaddr
Displays policies by MAC address.

mac *mac_address*
Selects a six-octet MAC address; for example, 00:50:56:8e:00:4b.

vms
Displays discovered VMs.

vss
Displays discovered standard virtual switches.

name
Selects a virtual switch.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the virtual assets configured on the vCenter and discovered on the VDX switch.

The switch interface column information is local to each switch in the fabric.

Examples

```
device# show vnetwork ?

Possible completions:
  datacenter Shows discovered datacenters
  diff       Shows vcenter and switch configuration diff
  dvpgs      Shows discovered distributed virtual port-groups
  dvs        Shows discovered distributed virtual switches
  hosts      Shows discovered hosts
  pgs        Shows discovered standard port-groups
  vcenter    Shows configured vCenter
  vmpolicy   Shows vnics/vmknics to portgroup to port-profile association
  vms        Shows discovered VMs
  vss        Shows discovered standard virtual switches

device# show vnetwork dvpgs

dvPortGroup                          dvSwitch                        Vlan
==================================== =============================== =========
ProductionVMs                        dvSwitch-Production             10-10,
dvSwitch-Production-DVUplinks-7589   dvSwitch-Production             0-4094,
switch# show vnetwork dvs

dvSwitch                      Host        Uplink Name    Switch Interface
========                      =========== ============== ================
dvSwitch-Production40         -           -              -
dvSwitch-Production41         -           -              -
Total Number of Entries: 2

device# show vnetwork hosts

Host                          Uplink Name  Uplink MAC       (d)Virtual Switch      Switch Interface
====                          ===========  =========         ================      ===============
ESX-4921.englab.brocade.com   vmnic0       e4:1f:13:43:54:90 vSwitch0              -
                              vmnic2       00:1b:21:8f:4a:f0 dvSwitch-Production   115/0/5
                              vmnic4       00:05:33:26:3e:ba vSwitch1              115/0/1
                              vmnic5       00:05:33:26:3e:bb dvSwitch-Production   -
ESX-4922.englab.brocade.com   vmnic0       e4:1f:13:43:95:5c vSwitch0              -
                              vmnic2       00:05:33:26:2d:90 dvSwitch-Production   115/0/10
                              vmnic3       00:05:33:26:2d:91 dvSwitch-Production   115/0/11
                              vmnic5       00:05:1e:eb:f9:94 vSwitch1              115/0/2

device# show vnetwork pgs

PortGroup    vSwitch         vlanId        Host
============ =============== ============= ============================
TestVMs      vSwitch1        50-50,        ESX-4922.englab.brocade.com
             vSwitch1        50-50,        ESX-4921.englab.brocade.com
VMkernel     vSwitch1        0-0,          ESX-4922.englab.brocade.com
             vSwitch1        0-0,          ESX-4921.englab.brocade.com
switch# show vnetwork vcenter status
vCenter          Start                Elapsed (sec)  Status
================ ==================== ============== ================
MYVC             2011-09-07 14:08:42  10             In progress


device# show vnetwork vmpolicy macaddr all

Associated MAC   Virtual Machine          (dv)PortGroup      Port-Profile
================ ======================== ================== ================
00:50:56:72:42:4c -                       ProductionVMs      auto-ProductionVMs
00:50:56:78:69:36 -                       VMkernel           auto-VMkernel
00:50:56:7b:e5:41 -                       ProductionVMs      auto-ProductionVMs
00:50:56:7d:96:16 -                       VMkernel           auto-VMkernel
00:50:56:8e:00:4b CentOS-4921             ProductionVMs      auto-ProductionVMs
00:50:56:8e:00:4d CentOS-4921             TestVMs            auto-TestVMs
00:50:56:8e:00:50 CentOS-4922             TestVMs            auto-TestVMs
00:50:56:8e:00:51 CentOS-4922             ProductionVMs      auto-ProductionVMs
switch# show vnetwork vms
```

```
Virtual Machine         Associated MAC    IP Addr     Host
======================= ================= =========== ======================
CentOS-4921             00:50:56:8e:00:4b -           ESX-4921.englab.brocade.com
                        00:50:56:8e:00:4d -           ESX-4921.englab.brocade.com
CentOS-4922             00:50:56:8e:00:50 -           ESX-4922.englab.brocade.com
                        00:50:56:8e:00:51 -           ESX-4922.englab.brocade.com
vSwitch           Host                            Uplink Name    Switch Interface
================= =============================== ============== ================
vSwitch0          djesxi-5064.englab.brocade.com vmnic0         -
                                                 vmnic1         -
                  ht-153.englab.brocade.com      vmnic0         -
                  ht-154.eng.brocade.com         vmnic0         -
vSwitch1          ht-153.englab.brocade.com      vmnic7         -
                  ht-154.eng.brocade.com         vmnic6         -
                                                 vmnic7         -
vSwitch2          ht-153.englab.brocade.com      vmnic6         -
Total Number of Entries: 8
```

History

Release version	Command history
5.0.2b	This command was introduced.
6.0.0	This command description was clarified.

show vrf

Displays VRF configuration information.

Syntax

show vrf

Modes

Privileged EXEC mode

show vrrp

Displays information about VRRP and VRRP-E sessions.

Syntax

show vrrp *VRID* [**detail**] [**summary**]

show vrrp detail

show vrrp interface *<N>* **gigabitethernet** *rbridge-id/slot/port* [**detail**] [**summary**]

show vrrp summary

Parameters

VRID

The virtual-group ID about which to display information. Valid values range from 1 to 128.

detail

Displays all session information in detail, including session statistics.

summary

Displays single line, session-information summaries.

interface

Displays information for an interface that you specify.

<N> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about VRRP and VRRP-E sessions, either in summary or full-detail format. Can also specify a particular virtual group or interface for which to display output.

This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** interface type. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples

To show all session information in detail, including session statistics:

```
switch# show vrrp detail

VRID 1
  Interface: Ten Gigabit Ethernet 0/18;  Ifindex: 403832850
  Mode: VRRP
  Admin Status: Enabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Master
  Virtual IP(s): 1.1.1.5, 1.1.1.6, 1.1.1.8, 1.1.1.9

  Configured Priority: 255  (default: 100); Current Priority: 255
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
  Statistics:
    Advertisements: Rx: 0, Tx: 10298
    ARP:            Rx: 0, Tx: 28
VRID 2
  Interface: Ten Gigabit Ethernet 0/22;  Ifindex: 404094998
  Mode: VRRP
  Admin Status: Disabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Initialize
  Virtual IP: unset
  Configured Priority: 100  (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
  Statistics:
    Advertisements: Rx: 0, Tx: 0
    ARP:            Rx: 0, Tx: 0
VRID 3
  Interface: Ten Gigabit Ethernet 0/18;  Ifindex: 403832850
  Mode: VRRP
  Admin Status: Enabled
  Address family: IPv4
  Authentication type: No Authentication
  State: Master
  Virtual IP(s): 1.1.1.20
  Configured Priority: 100  (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority
    =======                   ========
```

show zoning enabled-configuration

Displays information about the enabled zoning configuration.

Syntax

show zoning enabled-configuration

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the cfg-name and enabled-zone fields of the enabled zoning configuration for a Brocade VCS Fabric.

This command is supported in VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples

```
switch# show zoning enabled-configuration
zoning enabled-configuration cfg-name cfg1
zoning enabled-configuration enabled-zone zone1
 member-entry 10:00:00:00:00:00:00:01
zoning enabled-configuration enabled-zone zone2
 member-entry 10:00:00:00:00:00:00:02
switch# show zoning enabled-configuration | count
Count: 8 lines
```

Related Commands

show running-config zoning defined-configuration, show running-config zoning enabled-configuration

show zoning operation-info

Displays information about transactions and database size.

Syntax

show zoning operation-info

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge.

Command Output

The **show zoning operation-info** command displays the following information:

Output field	Description
db-max	Defines the maximum size in bytes of the zone database in nonvolatile memory.
db-avail	Displays the size in bytes of the unused portion of nonvolatile memory available for the defined configuration.
db-committed	Displays the size in bytes of the defined configuration currently stored in nonvolatile memory.
db-transaction	Displays the size in bytes of the uncommitted defined configuration.
db-token	Displays the current transaction token ID.
last-zone-changed-timestamp	Displays the last time the defined zone configuration was modified.
last-zone-committed-timestamp	Displays the data and time of the last time the zoning database was saved to nonvolatile memory.

Examples

To display information about transactions and database size:

```
switch# show zoning operation-info

db-max 1045274
db-avail 1043822
db-committed 440
db-transaction 0
transaction-token 0
last-zone-changed-timestamp 2011-11-16 14:38:15 GMT-7:00
last-zone-committed-timestamp 2011-11-16 14:38:15 GMT-7:00
```

Related Commands

show running-config zoning defined-configuration, show running-config zoning enabled-configuration, show zoning enabled-configuration

Commands shutdown through Z

shutdown

Disables the selected interface.

Syntax

shutdown

no shutdown

Command Default

The interface is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no shutdown** to enable the interface.

When an RBridge is rejoining the logical chassis cluster, the interface-level configuration is reset to the default values.

Examples

To disable a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 1/0/1
switch(conf-if-te-1/0/1)# shutdown
```

To enable a specific 1-gigabit Ethernet interface:

```
switch(config)# gigabitethernet interface 1/0/2
switch(conf-if-gi-1/0/2)# noshutdown
```

Related Commands

interface, interface ve, show interface, show ip interface

shutdown (STP)

Disables the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), the Spanning Tree Protocol (STP), Per Vlan Spanning Tree (PVST), or Rapid PVST(RPVST) globally.

Syntax

shutdown

no shutdown

Command Default

STP is not enabled as it is not required in a loop-free topology.

Modes

Protocol Spanning Tree configuration mode

Usage Guidelines

Enter **no shutdown** to re-enable all versions of STP.

Examples

To disable STP globally:

```
switch(config)# protocol spanning-tree rstp
switch(conf-rstp)# shutdown
```

To enable STP globally:

```
switch(config)# protocol spanning-tree rstp
switch(conf-rstp)# no shutdown
```

shutdown (UDLD)

Disables the unidirectional link detection (UDLD) protocol on all ports without affecting configuration.

Syntax

shutdown

no shutdown

Modes

Protocol UDLD configuration mode

Usage Guidelines

The **no shutdown** command unblocks all ports that have been blocked by the UDLD protocol.

Examples

To shutdown the UDLD protocol:

```
switch# configure
switch(config)# protocol udld
switch(config-udld)# shutdown
```

Related Commands

protocol udld

shutdown (VXLAN)

Administratively shuts down tunnels to a VXLAN overlay gateway site.

Syntax

shutdown

no shutdown

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

The **no shutdown** command enables tunnels to the site.

The "no shutdown" state for this mode is not displayed in the running configuration.

Examples

To shut down VXLAN overlay gateway tunnels:

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-overlay-gw-gateway1-site-mysite)# shutdown
```

Related Commands

overlay-gateway, site

shutdown-time

Specifies the delay between the time a port is disabled after Edge Loop Detection (ELD) detects a loop and the automatic re-enabling of that port.

Syntax

shutdown-time *num*

no shutdown-time *num*

Command Default

The default value is 0 minutes.

The port will not be re-enabled automatically.

Parameters

num

Specifies the number of minutes before a port is re-enabled. Valid values range from 10 through 1440 minutes (10 minutes to 24 hours).

Modes

ELD configuration mode

Usage Guidelines

NOTE

Any change to **shutdown-time** only takes effect for the ports that are disabled by ELD after the configuration change. Any ports that were already disabled by ELD before the **shutdown-time** change continues to follow the old **shutdown-time** value. These ports start to follow the new shutdown time after the currently running timer expires and ELD still detects the loop and shuts down the port again.

If you do not set a shutdown time using this command, you can re-enable all ELD-disabled ports manually using the **clear edge-loop-detection** command.

Enter **no shutdown-time** to return to the default value.

Examples

To re-enable ports 24 hours after they are disabled by ELD:

```
switch(config)# protocol edge-loop-detection

switch(config-eld)# shutdown-time 1440
```

To cancel automatic port re-enable:

```
switch(config-eld)# no shutdown-time 1440
```

Related Commands

clear edge-loop-detection, show edge-loop-detection globals, show edge-loop-detection rbridge-id

site

Creates a remote Layer 2 extension site in a VXLAN overlay gateway context and enables VXLAN overlay gateway site configuration mode.

Syntax

site *name*

no site *name*

Parameters

name

Site identifier. An ASCII character string up to 63 characters long, including the alphabet, numbers 0 through 9, hyphens (-), and underscores (_).

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

The VXLAN overlay gateway type must first be configured for Layer 2 extension, by means of the **type layer2-extension** command.

A "site" represents a remove VCS Fabric or the other end of the VXLAN tunnel. A site is associated with a "container," as data structure that includes the destination IPv4 address of the tunnel, the switchport VLANs, and the administrative state.

Use the **no site** command with a specified name to remove the tunnel that corresponds to the site.One you create the site instance, you enter VXLAN overlay gateway site configuration mode, where you can configure other properties for the site. The key commands available in this mode are summarized below:

TABLE 18 Key commands available in VXLAN overlay gateway site configuration mode

Command	Description
extend vlan	Configures switchport VLANs for the tunnels to the containing site in a VXLAN overlay gateway configurations.
ip address	Specifies the IPv4 address of a destination tunnel in VXLAN overlay gateway configurations.
shutdown	Administratively shuts down tunnels to a VXLAN overlay gateway site.

Examples

To create a VXLAN overlay gateway site and enter VXLAN overlay gateway site configuration mode:

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-overlay-gw-gateway1-site-mysite)#
```

Related Commands

overlay-gateway

slot

Enables or disables the slot.

Syntax

slot *number* { **disable** | **enable** }

Command Default

This command has no defaults.

Parameters

number

The slot to control. The valid values are 0 or 1.

disable

Disables the slot.

enable

Enables the slot.

Modes

Privileged EXEC mode

snmp trap link-status

Enables or disables SNMP traps for a particular interface.

Syntax

snmp trap link-status

no snmp trap link-status

Command Default

By default, the status is deactivated.

Modes

Interface configuration mode

Usage Guidelines

This command is only available for Network OS v5.0.2 and v5.0.2a.

Use the **no snmp trap link-status** command to deactivate the status.

The **snmp trap link-status** command is available for all interface speeds.

History

Release version	Command history
5.0.2	This command was introduced.

snmp-server community

Sets the community string and associates it with the user-defined group name to restrict the access of MIB for SNMPv1 and SNMPv2c requests.

Syntax

snmp-server community *string* [**groupname** *group-name*] [**ipv4-acl** *standard-ipv4-acl-name*] [**ipv6-acl** *standard-ipv6-acl-name*]

no snmp-server community *string* [**groupname** *group-name*] [**ipv4-acl** *standard-ipv4-acl-name*] [**ipv6-acl** *standard-ipv6-acl-name*]

Command Default

By default no group name is mapped with the community string. User must map the community string with any non-existing or existing group name to contact the switch through SNMPv1 or SNMPv2c.

Parameters

string
Specifies the community string.

groupname *group-name*
Specifies the group name associated with the community name.

ipv4-acl *standard-ipv4-acl-name*
Specifies an IPv4 ACL that contains rules permitting or denying access from specified IPv4 addresses.

ipv6-acl *standard-ipv6-acl-name*
Specifies an IPv6 ACL that contains rules permitting or denying access from specified IPv6 addresses.

Modes

Global configuration mode

Usage Guidelines

This command manages the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 and SNMPv2c configuration settings.

The maximum number of SNMP communities supported is 256.

Use a **no** form of this command to do one of more of the following:

- Remove the specified community string and all entities associated with it
- Remove the groupname from the string
- Remove the IPv4 ACL from the string
- Remove the IPv6 ACL from the string

Examples

The following example adds the community string "public" and associates the group name "user" with it.

```
switch(config)# snmp-server community public groupname user
switch(config)#
```

The following example also applies an IPv4 ACL and an IPv6 ACL.

```
switch(config)# snmp-server community comm1 groupname accGroup1 ipv4-acl standV4ACL1 ipv6-acl
standV6ACL1
switch(config)#
```

The following example removes the IPv4 and IPv6 ACLs from the "public" community.

```
switch(config)# no snmp-server community public ipv4-acl
switch(config)# no snmp-server community public ipv6-acl
```

History

Release version	Command history
5.0.2	This command was modified to apply ACLs that contains rules permitting or denying access from specified addresses.

snmp-server contact

Sets the SNMP server contact string.

Syntax

snmp-server contact *string*

no snmp-server contact *string*

Command Default

The default contact string is "Field Support."

Parameters

string

Specifies the server contact. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default values.

Examples

To set the SNMP server contact string to "Operator 12345":

```
switch(config)# snmp-server contact "Operator 12345"
```

To set the SNMP server contact string to the default of "Field Support":

```
switch(config)# no snmp-server contact
```

snmp-server context

Maps the context name in an SNMPv3 packet's protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance.

Syntax

snmp-server context *context_name* **vrf-name** *vrf_name*

no snmp-server-context *context_name* **vrf-name** *vrf_name*

Parameters

context

Enables the specification of a variable *context_name* that can be passed in the SNMP PDU.

vrf-name

Enables the specification of a variable *vrf_name* that can be retrieved when an SNMP request is sent with the configured *context_name*. This variable can be used in SNMP requests for "ipCidrRouteTable."

Modes

Global configuration mode

Usage Guidelines

The context-to-VRF mapping is one-to-one and is applicable to all SNMP versions.

Examples

The following **snmp-server context** command maps the context name "mycontext" to the VRF name "myvrf."

```
switch(config)# snmp-server context mycontext vrf-name myvrf
```

The following **snmp-server context** command deletes the VRF name "myvrf."

```
switch(config)# no snmp-server context mycontext vrf-name myvrf
```

The following **snmp-server context** command creates the new VRF name "mynewvrf"and maps the context to it.

```
switch(config)# snmp-server context mycontext vrf-name mynewvrf
```

snmp-server enable trap

This command controls the activation of the SNMP traps.

Syntax

snmp-server enable trap

no snmp-server enable trap

Command Default

The SNMP server traps are enabled by default.

Modes

Global configuration mode.

Usage Guidelines

Use the **no snmp-server enable trap** to disable the SNMP traps.

Examples

The following example activates the SNMP traps.

```
switch# configure terminal
switch(configure)# snmp-server enable trap
```

History

Release version	Command history
5.0.0	This command was introduced.

snmp-server engineid local

Configures a user-defined engine ID for the SNMP agent.

Syntax

snmp-server engineid local *engine_id*

no snmp-server engineid local

Modes

RBridge ID configuration mode

Usage Guidelines

A switch reboot is necessary for the configured engine ID to become active. Enter the **no snmp-server engineid local** command to remove the configured engine ID from database.

Examples

To configure a user-defined engine ID for the SNMP agent:

```
switch (config-rbridge-id-152)# snmp-server engineid local 10:00:00:05:33:51:A8:65:05:33:51:A8
```

To remove the configured engine ID from the database:

```
switch(config)# no snmp-server engineid local
switch (config-rbridge-id-152)# no snmp-server engineid local
```

snmp-server group

Creates user-defined groups for SNMPv1/v2/v3 and configures read, write, and notify permissions to access the MIB view.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

no snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

Command Default

Six default groups are supported to associate the default SNMPv3 user groups and the default SNMPv1/v2c community groups with the view configuration. The default group configurations are as follows:

```
switch(config)# snmp-server group admin v1 read All write All notify All
switch(config)# snmp-server group admin v2c read All write All notify All
switch(config)# snmp-server group snmpadmin v3 notify All
switch(config)# snmp-server group snmpuser v3 notify All
switch(config)# snmp-server group user v1 read All notify All
switch(config)# snmp-server group user v2c read All notify All
```

NOTE

By default, SNMPv3 groups "snmpadmin" and "snmpuser" are configured with noauth security level. Once the default SNMPv3 users are updated with auth and priv credentials then the corresponding group configuration needs to be updated with read/write view name. Also, the security level to access the switch through SNMPv3 user need to be updated, if required.

Parameters

groupname

Specifies the name of the SNMP group to be created.

v1 | **v2c** | **v3**

Specifies the version of SNMP.

auth | **noauth** | **priv**

Determines whether authentication is required for accessing the supported views. If auth is selected, then only authenticated packets with no privacy are allowed to access the specified view. If noauth is selected, then no authentication and no privacy are required to access the specified view. If priv is selected, then authentication and privacy are required from the users to access the view.

NOTE

These parameters are available only for SNMPv3 user groups.

read *viewname*

Specifies the name of the view that enables you to provide read access.

write *viewname*

Specifies the name of the view that enables you to provide both read and write access.

notify *viewname*

Specifies the name of the view that enables you to provide access to the MIB for trap or inform.

Modes

Global configuration mode

Usage Guidelines

Maximum number of SNMP groups supported is 10.

Examples

To create SNMP server group entries for SNMPv3 user group with auth/noauth permission:

```
switch(config)# snmp-server group group1 v3 auth read myview write myview notify myview
switch(config)# snmp-server group group2 v3 noauth read all write all notify all
switch(config)# snmp-server group group3 v3 auth
```

To remove the configured SNMP server groups:

```
switch(config)# no snmp-server group test1 v3 auth
switch(config)# no snmp-server group TEST1 v3 auth read myview write myview
switch(config)# no snmp-server group TEST2 v3 noauth read all write all notify all
```

snmp-server host

Configures the SNMP trap server host attributes.

Syntax

snmp-server host { **ipv4_host** | **ipv6_host** | **dns_host** } *community_string* [**version** { **1** | **2c** }] [**udp-port** *port*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf** { **mgmt-vrf** | **default-vrf** }] [{ **source-interface** *loopback_value* | **ve** *interface_id*}]

no snmp-server host { **ipv4_host** | **ipv6_host** | **dns_host** } *community_string* [**version** { **1** | **2c** }] [**udp-port** *port*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf** { **mgmt-vrf** | **default-vrf** }] [{ **source-interface** *loopback_value* | **ve** *interface_id*}]

Parameters

host { **ipv4_host** | **ipv6_host** | **dns_host** }
: Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

community_string
: Specifies the community string associated with the host entry.

version { **1** | **2c** }
: Selects version 1 or 2c traps to be sent to the specified trap host.

udp-port *port*
: Specifies the UDP port where SNMP traps will be received. Valid port IDs range from 0 through 65535. The default port is 162.

source-interface *loopback_value*
: Specifies the loopback port where SNMP traps will be received. Valid port IDs range from 1 through 255.

ve *interface_id*
: Specifies the VE port where SNMP traps will be received. Valid port IDs range from 1 through 8191.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }
: Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of **none** is specified, all traps are filtered and no RASLog traps are received.

use-vrf { **mgmt-vrf** | **default-vrf** }
: Configures SNMP to use the selected VRF to communicate with the host. This parameter is optional. The VRF name can be only two alphanumeric strings, "mgmt-vrf " and "default -vrf ". The default option is "mgmt-vrf ".

Modes

Global configuration mode

Usage Guidelines

This command sets the trap destination IP addresses and SNMP version, associates a community string with a trap host community string (for v1 and v2c), and specifies the UDP destination port where SNMP traps will be received.

To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The host supports six communities and their associated trap recipients and trap recipient severity levels. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string should be between 2 and 16 characters.

The **no snmp-server host** *host* **community-string** *string* **version 2c** command brings version 2c down to version 1.

The **no snmp-server host** *host* **community-string** *string* command removes the SNMP server host from the switch configuration altogether.

Examples

The following snmp-server host ipv6_host command creates an entry for trap host 1050:0:0:0:5:600:300c:326b associated with community "public." The trap host receives traps from the configured switch.

```
switch(config)# snmp-server host 1050:0:0:0:5:600:300c:326b public severity-level Info
```

The following snmp-server host dns_host command creates an entry for trap host brcd.brocade.com associated with community "public." The trap host receives traps from the configured switch.

```
switch(config)# snmp-server host brcd1.brocade.com public severity-level info
switch(config)# snmp-server v3host brocade.com snmpuser3 notifytype informs engineid 80:00:05:23:01:AC:
1A:01:F6 severity-level Info
```

To associate "commaccess" as a read-only community and set 10.32.147.6 as a trap recipient with SNMP version 2c on target port 162:

```
switch(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162
```

To create a trap host (10.23.23.45) associated with the community "public", which will receive all traps with the severity levels of Info, Warning, Error, and Critical:

```
switch(config)# snmp-server host 10.23.23.45 public severity-level info
```

To reset the severity level to None:

```
switch(config)# snmp-server host 10.23.23.45 public severity-level none
```

To associate a use-vrf for a trap host recipient:

```
switch(config)# snmp-server host 10.24.61.10 public use-vrf default-vrf
```

snmp-server location

Sets the SNMP server location string.

Syntax

snmp-server location *string*

no snmp-server location *string*

Command Default

The location string is "End User Premise."

Parameters

string

Specifies the SNMP server location string. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Examples

To set the SNMP server location string to "Building 3 Room 214":

```
switch(config)# snmp-server location "Building 3 Room 214"
```

To set the SNMP server location to the default, "End User Premise":

```
switch(config)# no snmp-server location
```

snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

Syntax

snmp-server sys-descr *string*

no snmp-server sys-descr

Command Default

The system description is "Brocade VDX switch".

Parameters

string

The text for the system description. The string must be between 4 and 255 characters in length.

Modes

Global configuration mode

Usage Guidelines

Enter **no snmp-server sys-descr** to return to the default system description.

Examples

To set the system description OID to "Brocade Cluster switch":

```
switch(config)# snmp-server sys-descr "Brocade Cluster switch"
```

To restore the system description OID to the default:

```
switch(config)# no snmp-server sys-descr
```

snmp-server user

Creates or changes the attributes of SNMPv3 users, and allows the SNMPv3 user to be associated with the user-defined group name.

Syntax

snmp-server user *username* [**groupname** *group-name*] [**auth** { **md5** | **sha** | **noauth** }] [**auth-password** *string* [**encrypted**]] [**priv** { **DES** | **AES128** | **nopriv** }] [**priv-password** *string* [**encrypted**]] [**ipv4-acl** *standard-ipv4-acl-name*] [**ipv6-acl** *standard-ipv6-acl-name*]

no snmp-server user *username* [**groupname** *group-name*] [**auth** { **md5** | **sha** | **noauth** }] [**auth-password** *string* [**encrypted**]] [**priv** { **DES** | **AES128** | **nopriv** }] [**priv-password** *string* [**encrypted**]] [**ipv4-acl** *standard-ipv4-acl-name*] [**ipv6-acl** *standard-ipv6-acl-name*]

Parameters

username
The name of the user that connects to the agent. The name must be between 1 and 16 characters long.

groupname *group-name*
The name of the group to which the user is associated. The configured user is allowed to be associated with the user-defined groups created using the **snmp-server group** command.

auth
Initiates an authentication level setting session. Default is **noauth**.

noauth
Removes authentication.

md5
The HMAC-MD5-96 authentication level.

sha
The HMAC-SHA-96 authentication level.

auth-password *string*
A string that enables the agent to receive packets from the host. Passwords are plain text and must be added each time for each configuration replay. The password must be between 1 and 32 characters long.

priv
Initiates a privacy authentication level setting session. Default is nopriv.

DES
Specifies the DES privacy protocol.

AES128
Specifies the AES128 privacy protocol.

nopriv
Removes privacy

priv-password *string*
A string (not to exceed 32 characters) that enables the host to encrypt the contents of the message that it sends to the agent. Passwords are plain text and must be added each time for each configuration replay. The privacy password alone cannot be configured. You configure the privacy password with the authentication password.

encrypted
Used to enter the input for auth/priv passwords as encrypted. The encrypted key should be used only while entering the encrypted auth/priv passwords.

ipv4-acl *standard-ipv4-acl-name*
Specifies an IPv4 ACL that contains rules permitting or denying access from specified IPv4 addresses.

ipv6-acl *standard-ipv6-acl-name*
Specifies an IPv6 ACL that contains rules permitting or denying access from specified IPv6 addresses.

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

This command configures SNMPv3 users that can be associated with a trap and inform response functionality. This command also allows configured user to be associated with user-defined SNMP groups created using the **snmp-server group** command. The maximum number of SNMP users that can be configured is 10. Optional encryption for **auth-password** and **priv-password** is also provided.

When creating a new SNMPv3 user without group name, by default there is no group name mapped with the SNMPv3 user. You must map the configured SNMPv3 user with any non-existing or existing group name available in the group CLI configuration to contact the switch through SNMPv3.

The behavior of this command in the local RBridge ID configuration is same as the global configuration. If the user name configured is same in both global and RBridge ID configurations, then the RBridge ID configuration will take precedence. The encrypted password generated in the global configuration can be used for another global user to modify the passwords. The encrypted passwords generated in global configurations cannot be used in the RBridge ID configurations and vice versa.

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

Use a **no** form of this command to do one of more of the following:

- Remove the specified user and all entities associated with it
- Remove the groupname from the user
- Remove the authorization protocol from the user
- Remove the privacy protocol from the user
- Remove the IPv4 ACL from the user
- Remove the IPv6 ACL from the user

Examples

The following example configures a basic authentication policy.

```
switch(config)# snmp-server user brocade groupname snmpadmin auth md5 auth-password user123 priv AES128
priv-password user456
```

The following example configures plain-text passwords.

```
switch(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv  DES priv-password
public123
```

The following example configures configure encrypted passwords.

```
switch(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password "MVb
+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
```

The following example creates the SNMP users "user1" and "user2" associated with used-defined group "group1" under global configuration mode.

```
switch(config)# snmp-server user user1 groupname group1
switch(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES priv-
password password
```

The following example configures an SNMPv3 user under local RBridge ID configuration mode.

```
switch(config-rbridge-id-1)# snmp-server user snmpadmin1 groupname snmpadmin auth sha auth-password
private123 priv DES priv-password public123
```

The following example configures the SNMPv3 users "user1" and "user2" associated with user-defined group "group1" under global configuration mode. It also applies an IPv4 ACL and an IPv6 ACL to "user1."

```
switch(config)# snmp-server user user1 groupname group1 ipv4-acl standV4ACL1 ipv6-acl standV6ACL1
switch(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES priv-
password
```

The following example removes groupname, the authentication and privacy protocols, and the IPv4 ACL from the user.

```
switch(config)# no snmp-server user user1 groupname snmpadmin auth sha priv DES ipv4-acl
```

History

Release version	Command history
5.0.2	This command was modified to apply ACLs that contains rules permitting or denying access from specified addresses.

snmp-server v3host

Specifies the recipient of the SNMPv3 notification parameter.

Syntax

snmp-server v3host [**host** { **ipv4_host** | **ipv6_host** | **dns_host**}] *user_name* [**notifytype** {**traps** | **informs**}] **engineid** *engine-id* **udp-port** *port_number* [**severity-level** | {**none** | **debug** | **info** | **warning** | **error** | **critical**}] [**use-vrf** { **mgmt-vrf** | **default-vrf** }] [{ **source-interface** *loopback_value* | **ve** *interface_id*}]

no snmp-server v3host [**host** { **ipv4_host** | **ipv6_host** | **dns_host**}] [**use-vrf** { **mgmt-vrf** | **default-vrf** }] [{ **source-interface** *loopback_value* | **ve** *interface_id*}]

Parameters

host { **ipv4_host** | **ipv6_host** | **dns_host** }
Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

user_name
Specifies the SNMPv3 user name to be associated with the SNMPv3 host entry.

notifytype { **traps** | **informs** }
Specifies the type of notification traps that are sent for the host. Traps and informs are supported. The default notify type is traps.

engineID *engine-id*
Configures the remote engine ID to receive informs on a remote host.

udp-port *port_number*
Specifies the UDP port of the host. The default UDP port number is 162.

source-interface *loopback_value*
Specifies the loopback port where SNMP traps will be received. Valid port IDs range from 1 through 255.

ve *interface_id*
Specifies the VE port where SNMP traps will be received. Valid port IDs range from 1 through 8191.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }
Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of None is specified, all traps are filtered and no RASLog traps are received. The default severity level is none.

use-vrf { **mgmt-vrf** | **default-vrf** }
Configures SNMP to use the selected VRF to communicate with the host. This parameter is optional. The VRF name can be only two alphanumeric strings, "mgmt-vrf " and "default -vrf ". The default option is "mgmt-vrf ".

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

The global SNMPv3 host can be configured by associating with only global SNMPv3 users and the local SNMPv3 host can be configured by associating with only local SNMPv3 users. You cannot create a SNMPv3 host in global configuration by associating with the local SNMPv3 users and vice versa.

Examples

The **snmp-server v3host** command is similar to the snmp-server host command.

To configure an IPv4 host address under global configuration mode:

```
switch(config)# snmp-server v3host 10.23.23.45 snmpadmin1 severity-level info
```

The following command creates an entry for SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2" under global configuration mode. The trap host will receive SNMPv3 traps from the configured switch.

```
switch(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2 severity-level Info
```

The following command creates an entry for SNMPv3 trap host 10.26.3.166 associated with SNMP user "snmpuser2" under RBridge ID configuration mode. The trap host will receive SNMPv3 traps from the configured switch.

```
switch(config-rbridge-id-1)# snmp-server v3host 10.26.3.166 snmpuser2 severity-level Info udp-port 4425
```

The following command removes the SNMPv3 trap host 10.26.3.166 associated with SNMP user "snmpuser2".

```
switch(config-rbridge-id-1)# no snmp-server v3host 10.26.3.166 snmpuser2
```

To associate a use-vrf for a trap host recipient.

```
switch(config)# snmp-server v3host 10.24.61.10 public use-vrf default-vrf
```

snmp-server view

Creates or removes a view entry with MIB objects to be included or excluded for user access.

Syntax

snmp-server view *view-name mib_tree* {**included** | **excluded**}

no snmp-server view *view-name mib_tree* {**included** | **excluded**}

Command Default

The default view configuration is "All" with base OID "1" (iso) included.

```
switch(config)# snmp-server view All 1 included
```

Parameters

view-name
: Specifies the alphanumeric name to identify the view. The name should not contain spaces.

mib_tree
: Specifies the MIB object ID called Object Identifiers (OIDs) that represent the position of the object or sub-tree in the MIB hierarchy.

included | **excluded**
: Specifies whether the MIB object ID identified by the *mib_tree* variable must be included in the view or excluded from the view.

Modes

Global configuration mode

Usage Guidelines

Maximum number of views supported with MIB tree entries is 10. Either a single view name associated with 10 different MIB object IDs or 10 different view names associated with each one of the MIB Object IDs is allowed.

Examples

To create a SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3":

```
switch(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

To create SNMP view entry "view2" with included permission for the MIB object ID "1.3.6.1":

```
switch(config)# snmp-server view view2 1.3.6.1 included
```

To remove the SNMP view entry "view1" from the configuration list:

```
switch(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

source

Configures the monitoring session.

Syntax

source [**fortygigabitethernet** *rbridge-id/slot/port* | *<N>***gigabitethernet** *rbridge-id/slot/port* | **destination** | **direction** [**rx** | **tx** | **both**]

no source [*<N>***gigabitethernet** *rbridge-id/slot/port* | **destination** | **direction** [**rx** | **tx** | **both**]

Parameters

*<N>***gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

destination

Use this parameter to specify the interface.

direction rx

Specifies to monitor the receiving traffic.

direction tx

Specifies to monitor the transmitting traffic

direction both

Specifies to monitor transmitting and receiving traffic.

Modes

Monitor session configuration mode

Usage Guidelines

Enter **no source** followed by the identifying parameters to delete the port mirroring connection for the specified interface.

Examples

To enable session 22 for monitoring traffic:

```
switch(config)# monitor session 22
switch(config-session-22)# source tengigabitethernet 0/1 destination tengigabitethernet 0/15 direction
both
```

Related Commands

monitor session

span session

Configures the SPAN session.

Syntax

span session *session_id*

no span session *session_id*

Parameters

session_id

Designates the session number for the flow-based SPAN session.

Modes

Policy class configuration mode

Usage Guidelines

Use the **no span session** *session-id* command to delete the session.

Related Commands

destination

spanning-tree autoedge

Enables automatic edge detection.

Syntax

spanning-tree autoedge

no spanning-tree autoedge

Command Default

Auto-detection is not enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.Enter **no spanning-tree autoedge** to disable automatic edge detection.

Examples

To enable automatic edge detection:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree autoedge
```

Related Commands

protocol spanning-tree

spanning-tree bpdu-mac

Sets the MAC address of the Bridge Protocol Data Unit (BPDU).

Syntax

spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

no spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

Parameters

0100.0ccc.cccd
: Cisco Control Mac

0304.0800.0700
: Brocade Control Mac

Modes

Interface subtype configuration mode

Usage Guidelines

This command will only take effect when the protocol is PVST+ or R-PVST+.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes. Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no spanning-tree bpdu-mac 0100.0ccc.cccd** to remove the address.

spanning-tree cost

Changes an interface's spanning-tree port path cost.

Syntax

spanning-tree cost *cost*

Command Default

The default path cost is 200000000.

Parameters

cost

Specifies the path cost for the Spanning Tree Protocol (STP) calculations. Valid values range from 1 through 200000000.

Modes

Interface subtype configuration mode

Usage Guidelines

Lower path cost indicates a greater chance of becoming root.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Examples

To set the port cost to 128:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree cost 128
```

Related Commands

show spanning-tree

spanning-tree edgeport

Enables the edge port on an interface to allow the interface to quickly transition to the forwarding state.

Syntax

spanning-tree edgeport [**bpdu-filter** | **bpdu-guard**]

Command Default

Edge port is disabled.

Parameters

bpdu-filter

Sets the edge port Bridge Protocol Data Unit (BPDU) filter for the port.

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is only for RSTP and MSTP. Use the **spanning-tree portfast** command for STP

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.Note the following details about edge ports and their behavior:

- A port can become an edge port if no BPDU is received.
- A port must become an edge port before it receives a BPDU.
- When an edge port receives a BPDU, it becomes a normal spanning-tree port and is no longer an edge port.
- Because ports directly connected to end stations cannot create bridging loops in the network, edge ports directly transition to the forwarding state, and skip the listening and learning states

Examples

To enable a port to quickly transition to the forwarding state:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree edgeport
```

To set the edgeport BPDU filter for the port:

```
switch(conf-if-te-0/1)# spanning-tree edgeport
switch(conf-if-te-0/1)# spanning-tree edgeport bpdu-filter
```

To guard the port against reception of BPDUs:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree edgeport
switch(conf-if-te-0/1)# spanning-tree edgeport bpdu-guard
```

Related Commands

spanning-tree portfast, spanning-tree autoedge

spanning-tree guard root

Enables the guard root to restrict which interface is allowed to be the spanning-tree root port or the path-to-the-root for the switch.

Syntax

spanning-tree guard root [**vlan** *vlan_id*]

no spanning-tree guard root

Command Default

Guard root is disabled.

Parameters

vlan *vlan_id*
Specifies a VLAN.

Modes

Interface subtype configuration mode

Usage Guidelines

Guard root protects the root bridge from malicious attacks and unintentional misconfigurations where a bridge device that is not intended to be the root bridge becomes the root bridge. This causes severe bottlenecks in the data path. Guard root ensures that the port on which it is enabled is a designated port. If the guard root enabled port receives a superior Bridge Protocol Data Unit (BPDU), it goes to a discarding state.

If the VLAN parameter is not provided, the guard root functionality is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

The root port provides the best path from the switch to the root switch.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes. Enter **no spanning-tree guard root** to disable guard root on the selected interface.

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples

To enable guard root:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree guard root
```

Related Commands

show spanning-tree

spanning-tree hello-time

Configures the hello-time in seconds on the interface.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Command Default

2 seconds.

Parameters

seconds

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent by the root switch configuration messages. Valid values range from 1 through 10.

Modes

Interface subtype configuration mode

Usage Guidelines

This command sets the interval time between the BPDUs sent by the root switch. This command is only for MSTP.

Changing the **hello-time** value affects all spanning-tree instances.

The **max-age** command setting must be greater than the **spanning-tree hello-time** command setting.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.Enter **no spanning-tree hello-time** to return to the default setting.

Examples

To set the hello time to 5 seconds:

```
switch(config)# interface tengigabitethernet 0/1

switch(conf-if-te-0/1)# spanning-tree hello-time 5
```

Related Commands

forward-delay, max-age, show spanning-tree

spanning-tree ieee-bpdu limit-vlan-flood

Restricts IEEE BPDU to within VLAN 4095.

Syntax

spanning-tree ieee-bpdu limit-vlan-flood

no spanning-tree ieee-bpdu limit-vlan-flood

Command Default

The IEEE BPDU is not restricted.

Modes

Rbridge ID configuration mode

Usage Guidelines

Use the **no spanning-tree ieee-bpdu limit-vlan-flood** command to remove the BPDU VLAN restriction.

When the device receives the IEEE BPDU on ingress port , it uses a ctrl-classifier entry that assigns the BPDU to the control VLAN 4095. It then broadcasts the BPDU on all edge ports, regardless of VLAN. However in an VF environment flooding should be limited. This command restricts the BPDU to VLAN 4095 and prevents flooding.

Examples

Typical command example

```
device(config-rbridge-id-158)# spanning-tree ieee-bpdu limit-vlan-flood
```

History

Release version	Command history
5.0.2b	This command was introduced.

spanning-tree instance

Sets restrictions for the port of particular MSTP instances.

Syntax

spanning-tree instance *instance_id* [**cost** *cost* | **priority** *priority* | **restricted-role** | **restricted-tcn**]

no spanning-tree instance *instance_id*

Command Default

The path-cost value is 2000 on a 10-gigabit Ethernet interface.

Parameters

instance_id
Specifies the MSTP instance. Valid values range from 1 through 32.

cost *cost*
Specifies the path-cost for a port. Valid values range from 1 through 20000000.

priority *priority*
Specifies the port priority for a bridge in increments of 16. Valid values range from 0 through 240.

restricted-role
Specifies to restrict the role of a port.

restricted-tcn
Specifies to restrict the propagation of the topology change notifications from a port.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command for MSTP-specific configurations.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Enter **no spanning-tree instance** *instance_id* to remove the specified MSTP instance.

Examples

To set restrictions for the port of MSTP instance 1 with the cost of 40000:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree instance 1 cost 40000
```

Related Commands

instance, show spanning-tree

spanning-tree link-type

Enables and disables the rapid transition for the Spanning Tree Protocol (STP).

Syntax

spanning-tree link-type [**point-to-point** | **shared**]

Command Default

The **spanning-tree link-type** is set to **point-to-point**.

Parameters

point-to-point
Enables rapid transition.

shared
Disables rapid transition.

Modes

Interface subtype configuration mode

Usage Guidelines

This command overrides the default setting of the link type.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Examples

To specify the link type as shared:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/0)# spanning-tree link-type shared
```

spanning-tree portfast

Enables the Port Fast feature on an interface to allow the interface to quickly transition to forwarding state.

Syntax

spanning-tree portfast [**bpdu-filter** | **bpdu-guard**]

Command Default

Port Fast is disabled.

Parameters

bpdu-filter

Sets the Port Fast BPDU filter for the port.

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is applicable the only for the Spanning Tree Protocol (STP). Port Fast immediately puts the interface into the forwarding state without having to wait for the standard forward time. Use the **spanning-tree edgeport** command for MSTP and RSTP.

BPDU filter prevents the switch from sending BPDU frames on ports that are enabled with portfast.

BPDU guard disables all portfast-enabled ports should they ever receive BPDU frames. It does not prevent transmitting of BPDU frames.

If you enable **spanning-tree portfast bpdu-guard** on an interface and the interface receives a BPDU, the software disables the interface and puts the interface in the ERR_DISABLE state.

Enable Port Fast on ports connected to host. Enabling Port Fast on interfaces connected to switches, bridges, hubs, and so on can cause temporary bridging loops, in both trunking and nontrunking mode.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Examples

To enable a port to quickly transition to the forwarding state:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast
```

To set the Port Fast BPDU filter for the port:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast bpdu-filter
```

To guard the port against the reception of BPDUs:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree portfast bpdu-guard
```

Related Commands

show spanning-tree, spanning-tree autoedge, spanning-tree edgeport

spanning-tree priority

Changes an interface's spanning-tree port priority.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Command Default

The default value is 128.

Parameters

priority

Specifies the interface priority for the spanning tree. The range of valid values is from 0 through 240. Port priority is in increments of 16.

Modes

Interface subtype configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all the RBridges.

Enter **no spanning-tree priority** to return to the default setting.

Examples

To configure the port priority to 16:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree priority 16
```

Related Commands

show spanning-tree, spanning-tree cost

spanning-tree restricted-role

Restricts the role of the port from becoming a root port.

Syntax

spanning-tree restricted-role

no spanning-tree restricted-role

Command Default

The restricted role is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all the RBridges.

Enter **no spanning-tree restricted-role** to return to the default setting.

Examples

To configure the port from becoming a root port:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree restricted-role
```

Related Commands

show spanning-tree

spanning-tree restricted-tcn

Restricts the Topology Change Notification (TCN) Bridge Protocol Data Units (BPDUs) sent on the port.

Syntax

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Command Default

The restricted TCN is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no spanning-tree restricted-tcn** to disable this parameter.

If xSTP is enabled over VCS, this command must be executed on all the RBridges.

Examples

To restrict the TCN on a specific interface:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree restricted-tcn
```

Related Commands

show spanning-tree

spanning-tree shutdown

Enables or disables spanning tree on the interface or VLAN.

Syntax

spanning-tree shutdown

no spanning-tree shutdown

Command Default

Spanning tree is disabled by defaut.

Modes

Interface subtype configuration mode

Usage Guidelines

Once all of the interfaces have been configured for a VLAN, you can enable Spanning Tree Protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently selected is used by the VLAN. Only one type of STP can be active at a time.

A physical interface (port) can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP enabled and VLAN 55 can have STP disabled simultaneously.

If xSTP is enabled over VCS, this command must be executed on all the RBridges.

Enter **no spanning-tree shutdown** to enable spanning tree on the interface or VLAN.

Vlan 1002 can not be enabled with the **spanning-tree shutdown** command while the device is in VCS Fabric mode.

Examples

To disable spanning tree on a specific interface:

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if-te-0/1)# spanning-tree shutdown
```

To enable spanning tree on VLAN 1002:

```
switch(config)# interface vlan 1002
switch(conf-if-vl-1002)# no spanning-tree shutdown
```

Related Commands

protocol spanning-tree

spanning-tree vlan

Configures the VLAN identifier for the spanning tree interface.

Syntax

spanning-tree vlan *vlan_id*

no spanning-tree vlan

Parameters

vlan *vlan_id*
Sets the VLAN identifier for the spanning tree interface.

Modes

Interface subtype configuration mode

Usage Guidelines

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Enter **no spanning-tree vlan** to remove the VLAN setting.

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Related Commands

forward-delay, max-age, show spanning-tree

speed (Ethernet)

Sets the speed negotiation value on an Ethernet interface.

Syntax

speed { **100** | **1000** | **1000-auto** | **10000** | **auto** }

no speed

Command Default

Speed is **auto**.

Parameters

100
Forces the speed to 100 Mbps.

1000
Forces the speed to 1 Gbps.

1000-auto
Forces the speed to 1 Gbps AN (802.3 Clause 37 Auto-Negotiation)

10000
Forces the speed to 10 Gbps.

auto
Allows the interface to negotiate the speed setting.

Modes

Interface subtype configuration mode

Usage Guidelines

The speed command is not available for 1-gigabit Ethernet or 40-gigabit Ethernet ports.

Enter **no speed** to return to the default.

Examples

To set the speed to 10 Gbps on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 170/0/1

switch(conf-if-int-170/0/1)# speed 10000
```

Related Commands

interface

speed (Fibre Channel)

Sets the operational speed on a Fibre Channel port.

Syntax

speed { **auto** | **1gbps** | **2gbps** | **4gbps** | **8gbps** }

Command Default

Speed is **auto** .

Parameters

auto
Allows the interface to negotiate the port speed.

2gbps
Sets the operational port speed to 2 Gbps.

4gbps
Sets the operational port speed to 4 Gbps.

8gbps
Sets the operational port speed to 8 Gbps.

16gbps
Sets the operational port speed to 16 Gbps.

Modes

Interface subtype configuration mode

Usage Guidelines

The Fibre Channel version of this command can be used only on Network OS platforms with Fibre Channel Flexports (Brocade VDX 6740 and Brocade VDX 2740) in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples

To set the Fibre Channel port speed:

```
switch (config)# interface FibreChannel 7/0/2

switch(conf-FibreChannel-7/0/2)# speed 4gbps
```

speed (FlexPort)

This command sets the protocol and speed for the FlexPort connector group.

Syntax

speed { **LowMixed** | **HighMixed** | **FibreChannel**}

Command Default

The default state is Ethernet.

Parameters

LowMixed

Sets to speed to 2/4/8G Fibre Channel and Ethernet speeds.

HighMixed

Sets the speed to 16G Fibre Channel and Ethernet speeds

FibreChannel

Sets the speed to support only fibre channel speeds and protocol. All FlexPorts in this connector-group must be converted to fibre-channel in order to use the FibreChannel connector-group speed.

Modes

Hardware connector-group configuration mode.

Usage Guidelines

None.

Examples

This example configures the speed for the FlexPort on Rbridge-ID 47, connector group 6, to support Fibre Channel.

```
switch(conf-if-fi-47/0/8)#speed FibreChannel
```

History

Release version	Command history
5.0.0	This command was introduced.

Related Commands

connector-group, flexport, hardware

speed (LAG)

Sets the speed on a LAG interface.

Syntax

speed { **1000** | **10000** | **40000** }

Command Default

Speed is 10000

Parameters

1000

Forces the speed to 1 Gbps.

10000

Forces the speed to 10 Gbps.

40000

Forces the speed to 40 Gbps.

Modes

Interface subtype configuration mode

Usage Guidelines

The speed command is available only for 10-gigabit Ethernet ports.

speed (port-channel)

Sets the speed on a port-channel interface.

Syntax

speed { **1000** | **10000** | **40000** | **100000** }

no speed

Command Default

Speed is 10000.

Parameters

1000

Forces the speed to 1 Gbps.

10000

Forces the speed to 10 Gbps.

40000

Forces the speed to 40 Gbps.

100000

Forces the speed to 100 Gbps. This is available only if the HundredGigabit line card is supported.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no speed** to return to the default setting.

Examples

To set the speed to 40 Gbps on a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-Port-Channel-44)# speed 40000
```

Related Commands

interface

spt-threshold

Configures the Shortest Path Tree (SPT) threshold.

Syntax

spt-threshold { **infinity** | *num* }

no spt-threshold

Command Default

Default value is 1.

Parameters

infinity

Use only the rendezvous point to send packets, do not switch over to SPT.

num

Rate (in kilobytes per second) that must be reached before switching to SPT. Valid values range from 1 through 4294967295.

Modes

PIM router configuration mode

Usage Guidelines

This command sets the rate, in kilobytes per second, data is to be sent through the rendezvous point before switching to SPT for sending packets.

Enter **no spt-threshold** to return to the default setting of 1.

Examples

To set the SPT threshold interval to 20:

```
switch(conf-pim-router)# spt-threshold 20
```

Related Commands

router pim

ssh

Connects to a remote server by means of the Secure Shell (SSH) protocol.

Syntax

ssh { *IP_address* | *hostname* } [**-c** | **-l** | **-m** | **interface** {*<N>***gigabitethernet** | **management** | **ve** *vlan-id* } | **vrf** *vrf_name*] }

Command Default

SSH connects to port 22.

Parameters

IP_address

Specifies the server IP address in IPv4 or IPv6 format.

hostname

Specifies the host name, a string from 1 through 253 characters.

-c

Specifies the encryption algorithm for the SSH session. This parameter is optional; if no encryption algorithm is specified, the default (**3des**) is used. Supported algorithms include the following:

3des

Triple Data Encryption Standard (DES). This is the default setting.

aes128-cbc

AES 128-bits

aes192-cbc

AES 192-bits

aes256-cbc

AES 256-bits

-l *username*

Login name for the remote server. This parameter is optional. If you specify a user name, you will be prompted for a password. If you do not specify a user name, the command assumes you are logging in as root and will prompt for the root password.

-m

Specifies the HMAC (Hash-based Message Authentication Code) message encryption algorithm. This parameter is optional; if no encryption algorithm is specified, the default (**hmac-md5**) is used. Supported algorithms include the following:

hmac-md5

MD5 128-bits. This is the default setting.

hmac-md5-96

MD5 96-bits

hmac-sha1

SHA1 160-bits

hmac-sha1-96
SHA1 96-bits

interface
Specifies an interface.

<N> **gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter **?** to see which interface subtypes are available. Replace *<N>***gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

management
Specifies a management interface.

ve *vlan-id*
Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

vrf *vrf-name*
Specifies a VRF instance. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to establish an encrypted SSH connection from a switch to a remote networking device. This implementation is based on SSH v2.

ATTENTION
Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management.

To use the **ssh** command on the management VRF, use the **vrf** keyword and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually.

```
switch# ssh vrf mgmt-vrf
```

The following features are not supported:

- Displaying SSH sessions
- Deleting stale SSH keys

Examples

To connect to a remote device using an SSH connection with default settings:

```
switch# ssh 10.70.212.152

The authenticity of host '10.70.212.152 (10.70.212.152)' can't be established.
RSA key fingerprint is f0:2a:7e:48:60:cd:06:3d:f4:44:30:2a:ce:68:fe:1d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.70.212.152' (RSA) to the list of known hosts.
Password:
```

To connect to a remote device using an SSH connection with a login name:

```
switch# ssh -l admin 127.2.1.8

admin@127.2.1.8's password
```

ssh client cipher non-cbc

Sets the SSH client's cipher list to non-cbc ciphers for the SSH client.

Syntax

ssh client cipher non-cbc

no ssh client cipher non-cbc

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no ssh client cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH client's cipher list to non-cbc ciphers, such as aes256-ctr, aes192-ctr, or aes128-ctr.

```
switch(config-rbridge-id-1)# ssh client cipher non-cbc
switch(config-rbridge-id-1)# do show running-config rbridge-id ssh
rbridge-id 1
ssh server non-cbc
ssh client non-cbc
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

ssh server cipher non-cbc

ssh server cipher non-cbc

Sets the SSH server's cipher list to non-cbc ciphers for the SSH server.

Syntax

ssh server cipher non-cbc

no ssh server cipher non-cbc

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no ssh server cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH server's cipher list to non-cbc ciphers, such as aes256-ctr, aes192-ctr, or aes128-ctr.

```
switch(config-rbridge-id-1)# ssh server cipher non-cbc
switch(config-rbridge-id-1)# do show running-config rbridge-id ssh
rbridge-id 1
ssh server non-cbc
ssh client non-cbc
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

ssh client cipher non-cbc

ssh server key

Generates or zeroizes SSH crypto keys on the device. All three keys can be active simultaneously.

Syntax

ssh server key {**dsa** | **rsa** [**1024** | **2048**] | **ecdsa 256**}

no ssh server key {**dsa** | **rsa** | **ecdsa**}

Command Default

The default values of SSH keys are:

- DSA is active
- ECDSA value is 256
- RSA value is 2048

Parameters

dsa
Generates the DSA key.

rsa [**1024** | **2048**]
Generates the RSA key, in either the 1024 or 2048 bit size.

ecdsa 256
Generates the ECDSA key at 256 bits.

Modes

RBridge ID configuration mode

Usage Guidelines

The **no ssh server key** command zeroizes the SSH keys on the device.

If you generate and delete SSH crypto keys, you must restart the SSH server using the **no ssh server shutdown** command to enable the configuration.

Earlier versions of Network OS have rsa, dsa and ecdsa keys, so after upgrading to Network OS v5.0.1a, respective entries are added into the configuration.

If you downgrade your device to a release earlier than Network OS v5.0.1a, the RSA, DSA, and ECDSA keys are generated if they do not exist.

Examples

Typical DSA command example:

```
switch(config-rbridge-id-176)# ssh server key dsa
```

Typical RSA command example:

```
switch(config-rbridge-id-176)#  ssh server key rsa 1024
```

Typical ECDSA command example:

```
switch(config-rbridge-id-176)#  ssh server key ecdsa 256
```

Typical zeroizing example:

```
switch(config-rbridge-id-176)# no ssh server key dsa
```

History

Release version	Command history
5.0.1a	This command was introduced.

ssh server key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

Syntax

ssh server key-exchange diffie-hellman-group14-sha1

no ssh server key-exchange

Command Default

This command is not configured by default.

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

You can configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh server key-exchange** to restore SSH server key-exchange to the default value.

This command is not distributed across the cluster. The RBridge ID of the node should be used to configure service on individual nodes.

For information on DH Group 14, refer to RFC 3526.

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

Examples

To set SSH server key-exchange to DH Group 14:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# ssh server key-exchange diffie-hellman-group14-sha1
```

To restore the SSH server key-exchange to default value:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no ssh server key-exchange
```

Related Commands

show running-config ssh server, show ssh server status

ssh server rekey-interval

Configures the Secure Shell (SSH) server rekey-interval.

Syntax

ssh server rekey-interval *interval*

no ssh server rekey-interval

Parameters

interval

The value for the rekey interval. Range is from 900 to 3600 seconds.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server rekey-interval** command to remove the rekey-interval.

ssh server shutdown

Disables SSH service on the switch.

Syntax

ssh server shutdown

no ssh server shutdown

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

Enter **no ssh server shutdown** to enable SSH service. This command is not distributed across the cluster. The RBridge ID of the node should be used to configure service on individual nodes.

Examples

To shut down SSH service:

```
switch(config)# rbridge-id-3
switch(config-rbridge-id-3)# ssh server shutdown
```

To enable SSH service:

```
switch(config-rbridge-id-3)# no ssh server shutdown
```

Related Commands

show support, telnet server shutdownshow running-config ssh server, show ssh server status

ssh server standby enable

Enables the SSH services on the standby MM.

Syntax

ssh server standby enable

no ssh server standby enable

Command Default

The SSH services are disabled on the standby MM.

Modes

RBridge ID configuration mode

Usage Guidelines

The **no ssh server standby enable** command disables the SSH services on the standby MM.

It is mandatory to specify the default-config when converting from Logical Chassis mode to Fabric Cluster mode, or the other way around. After conversion, the SSH and Telnet services on the standby MMs are disabled. This command enables the SSH services on the standby MM. .

Examples

Typical command output:

```
switch(config-rbridge-id-1)# no ssh server standby enable
switch(config-rbridge-id-1)# do show running-config rbridge-id | include standby
% No entries found.
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

telnet server standby enable

ssh server status

Displays SSH service on the switch.

Syntax

ssh server status

Modes

Global configuration mode

Examples

Typical command output:

```
switch# ssh server status
SSH Kex Exchange Algorithm: DH Group 14
```

Related Commands

show running-config ssh server, show ssh server status

static-network

Configures a static BGP4 network, creating a stable network in the core.

Syntax

static-network

no static-network *network/mask* [**distance** *num*]

Command Default

The default is 200.

Parameters

network/mask

Network and mask in CIDR notation.

num

Administrative distance value for this network. The range is from 1 through 255.

Modes

BGP address-family IPv4 unicast configuration mode

Usage Guidelines

While a route configured with this command will never flap unless it is deleted manually, a static BGP4 network will not interrupt the normal BGP4 decision process on other learned routes that are installed in the Routing Table Manager (RTM). Consequently, when there is a route that can be resolved, it will be installed into the RTM.

Use the **no** form of the command to restore the defaults.

Examples

Typical example of this command.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# static-network 10.11.12.0/24 distance 300
```

Related Commands

route-map

storm-control ingress

Limits ingress traffic on a specified interface.

Syntax

storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } { **limit-bps** | **limit-percent** } *rate* [{ **monitor** | **shutdown**] }

no storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } { **limit-bps** | **limit-percent** } *rate* [{ **monitor** | **shutdown**] }

Parameters

broadcast
Specifies that the command will operate on broadcast traffic only.

unknown-unicast
Specifies that the command will operate on unknown-unicast traffic only.

multicast
Specifies that the command will operate on multicast traffic only.

limit-bps
Specifies that the value given to the *rate* parameter is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface.

limit-percent
Specifies that the value given to the *rate* parameter is in percentage of capacity of the interface. If the traffic on the interface reaches this percentage of capacity, no more traffic (for the traffic type specified) is allowed on the interface.

rate
Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which parameter was chosen with the rate.

- Range if you are specifying rate in bps: 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate.
- Range if you are specifying rate in percent of interface capacity: 0 to 100.

monitor
Specifies that, if a rate limit is reached within a five-second sampling period, a log message gets sent. A log message is generated upon the first occurrence of such an event. Subsequent log messages are generated only at the end of one complete sample interval in which no rate limits are reached.

shutdown
Specifies that, if a rate limit is exceeded within a five-second sampling period, the interface will be shut down. You must manually re-enable the interface after a shutdown.

Modes

Interface subtype configuration mode

Usage Guidelines

This command limits the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic on a specified interface. The *shutdown* parameter monitors the status of the configured rate limit every five seconds, and if the maximum defined rate is exceeded the corresponding interface is shut down until you re-enable it using the **no shut** command.

This command is supported on the Brocade VDX 6740 6740, Brocade VDX 8770-4 and Brocade VDX 8770-8 platforms only.

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on an interface.

Examples

To configure storm control on a 10-gigabit Ethernet interface 101/0/2, with a limit-rate of 1000000 bps:
switch (config)# interface tengigabitethernet 101/0/2 switch (conf-if-te-101/0/2)# storm-control ingress broadcast 1000000

To disable BUM storm control for broadcast traffic only, on a 10-gigabit Ethernet interface 101/0/2:

```
switch (config)# int te 101/0/2
switch (conf-if-te-101/0/2)# no storm-control ingress broadcast
```

Related Commands

clear counters storm-control, interface, show storm-control

summary-address (OSPF)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *A.B.C.D E.F.G.H*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A.B.C.D E.F.G.H

IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPF VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

You can configure up to 32 address ranges. The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.This parameter affects only imported, type 5 external routes.

Enter **no summary-address** to disable route summarization.

Examples

To configure a summary address of 10.1.0.0 with a mask of 255.255.0.0:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# summary-address 10.1.0.0 255.255.0.0
```

NOTE

The command in this example configures summary address 10.1.0.0, which includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs.

summary-address (OSPFv3)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *A:B::C:D/LEN*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A:B:C:D/LEN
IPv6 summary address

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

You can configure up to 4 address ranges. The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

Examples

To configure a summary address of 2001:db8::/24 for routes redistributed into OSPFv3:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# summary-address 2001:db8::/24
```

NOTE

this example, the summary prefix 2001:db8::/24 includes addresses 2001:db8::/1 through 2001:db8::/24. Only the address 2001:db8::/24 is advertised in an external link-state advertisement.

support autoupload enable

Specifies if support autoupload is enabled or disabled. When set to enabled, the data files are automatically transferred to the configured remote location.

Syntax

support autoupload enable

no support autoupload enable

Command Default

Support autoupload is disabled by default.

Modes

Global configuration mode

Usage Guidelines

Whenever a core file, FFDC, trace data file occurs, the data files are automatically transferred to the configured remote location if the autoupload feature is enabled.

Use the **no** form of this command to disable support autoupload.

Examples

To enable autoupload mode:

```
switch(config)# support autoupload enable
```

To disable autoupload mode:

```
switch(config)# no support autoupload enable
```

support autoupload-param

Defines autoupload parameters.

Syntax

support autoupload-param hostip *host-ip* **user** *user_acct* **password** *password* **protocol** [**ftp** | **scp** | **sftp**] **directory** *path*

Parameters

hostip *host-ip*
Specifies the IP address of the remote host.

user *user_acct*
Specifies the user name to access the remote host.

password *password*
Specifies the password to access the remote host.

protocol FTP | SCP | SFTP
Specifies the protocol used to access the remote server.

directory *path*
Specifies the path to the directory.

rbridge-id
Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id
Specifies a unique identifier for a node.

all
Specifies all identifiers for a node.

Modes

Global configuration mode

Examples

To configure autoupload parameters:

```
switch(config)# support autoupload-param hostip 10.31.2.27 protocol [ftp|scp | sftp]username hegdes
directory /uers/home40/hegdes/autoupload password

(<string>): *****
```

support support-param

Defines support parameters.

Syntax

support support-param hostip *host-ip* **user** *user_acct* **password** *password* **protocol** [**ftp** | **scp** | **sftp**] **directory** *path*

Parameters

hostip *host-ip*
Specifies the IP address of the remote host.

user *user_acct*
Specifies the user name to access the remote host.

password *password*
Specifies the password to access the remote host.

protocol FTP | **SCP** | **SFTP**
Specifies the protocol used to access the remote server.

directory *path*
Specifies the path to the directory.

Modes

Global configuration mode

Examples

To configure support parameters:

```
switch(config)# support support-param hostip 10.31.2.27 protocol [ftp|scp | sftp]username hegdes
directory /uers/home40/hegdes/support password

(<string>): *****
```

switch-attributes

Sets switch attributes.

Syntax

switch-attributes *rbridge-id*

chassis-name *string*

host-name *string*

no switch-attributes

Command Default

The default chassis name depends on the switch model. You can assign the chassis name any name you wish to represent one of the following product names:

- VDX 6740
- VDX 6740T
- VDX 67440T-1G
- VDX 8770-4
- VDX 8770-8

The default host name is "sw0".

Parameters

rbridge-id

Specifies the RBridge ID the attribute is to be set for. Only the local RBridge ID is supported.

chassis-name *string*

Sets the switch chassis name. The string must be between 1 and 30 ASCII characters in length, and the leading character must be a letter.

host-name *string*

Sets the switch host name. The string must be between 1 and 30 ASCII characters in length, and the leading character must be a letter.

Modes

Global configuration mode

Usage Guidelines

When issued with the RBridge ID of the switch to be configured, this command goes into a sub-command shell where you can configure the host name or chassis name.

The text string for the **chassis-name** and **host-name** string is limited to 30 characters. The string must begin with a letter, and can consist of letters, digits, hyphens, periods (dots), and underscore characters. Spaces are not permitted.

This command is not supported on the standby management module.

This command is supported only on the local switch.

Enter **no switch-attributes** to restore the default values.

Examples

To set the host name for a switch with an RBridge ID of 2:

```
switch(config)# switch-attributes 2
switch(config-switch-attributes-1)# host-name VDX8770-4
```

Related Commands

show running-config switch-attributes

switchport

Puts the interface in Layer 2 mode and sets the switching characteristics of the Layer 2 interface. .

Syntax

switchport

no switchport

Command Default

All Layer 2 interfaces are mapped to default VLAN 1 and the interface is set to access mode.

Modes

Interface subtype configuration mode

Usage Guidelines

For changing the interface configuration mode to trunk or changing the default VLAN mapping, use additional **switchport** commands.

Enter **no switchport** to take the switch out of the Layer 2 mode.

Examples

To put a specific 10-gigabit Ethernet interface in Layer 2 mode:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport
```

To remove a specific port-channel interface from Layer 2 mode:

```
switch(config)# interface port-channel 44
switch(config-port-channel-44)# no switchport
```

switchport access

Sets the Layer 2 interface as access.

Syntax

switchport access { **vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id* }

no switchport access { **vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id* }

Command Default

All Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Parameters

vlan *vlan_id*
: Sets the port VLAN (PVID) to the specified *vlan_id*. Range is below 4096 for 802.1Q VLANs, and from 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

rspan-vlan *vlan_id*
: Sets a VLAN ID for RSPAN (Remote Switched Port Analyzer) traffic analysis.

mac *HHHH.HHHH.HHHH*
: Sets a source MAC address for classifying an untagged VLAN specified by the **vlan** keyword.

mac-group *mac-group-id*
: (Optional) Specifies a set of MAC addresses. The group of addresses must be established by the global **mac-group** command.

Modes

Interface subtype configuration mode on edge ports

Usage Guidelines

In access mode, the interface only allows untagged and priority tagged packets.

In a Virtual Fabrics context, use this command also to configure service or transport VFs on an access port. This allows multiple untagged VLANs on the port by means of SRC MAC classifiers.

Enter **no switchport access vlan** to set the PVID to the default VLAN 1.

Examples

To set the Layer 2 interface PVID to 100 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport access vlan 100
```

To set the PVID to the default VLAN 1 on a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-port-channel-44)# no switchport access vlan
```

The following examples illustrate configuration with service or transport VFs in a Virtual Fabrics context.

In global configuration mode, establish a mac-group:

```
switch(config)# mac-group 1
switch(config-mac-group 1)# mac 0002.0002.0002
switch(config-mac-group 1)# mac 0005.0005.0005
switch(config-mac-group 1)# mac 0008.0008.0008
```

In interface configuration mode, ensure that the switchport mode is set to access:

```
switch(config)# int te 2/0/1
switch(config-if-te-2/0/1)# switchport mode access
```

Set the default access VLAN (the default is 1) to 5000 (a classified VLAN):

```
switch(config-if-te-2/0/1)# switchport access vlan 5000
```

Classify an 802.1Q VLAN by means of a source MAC address:

```
switch(config-if-te-2/0/1)# switchport access vlan 200 mac 0002.0002.0002
```

Configure a classified VLAN (> 4095) on the same interface with a MAC address. Frames that do not match the source MAC addresses of 0002.0002.0002 or 0004.0004.0004 are classified into VLAN 5000 (the access VLAN for all untagged frames that do not have MAC address classifications.

```
switch(config-if-te-2/0/1)# switchport access vlan 6000 mac 0004.0004.0004
```

The following errors occur because a MAC address can be classified to only one VLAN on the same interface.

```
switch(config-if-te-2/0/1)# switchport access vlan 7000 mac-group 1
switch(config-if-te-2/0/1)# %Error: Mac-address/Mac-group is overlapping with another Mac-address/Mac-
group configuration on the same port.
switch(config-if-te-3/0/1)# switchport mode access
switch(config-if-te-3/0/1)# switchport access vlan 7000 mac-group 1
switch(config-if-te-3/0/1)# switchport access vlan mac 8000 0008.0008.0008
switch(config-if-te-3/0/1)# %Error: Mac-address/Mac-group is overlapping with another Mac-address/Mac-
group configuration on the same port.
```

switchport mode

Sets the mode of the Layer 2 interface.

Syntax

switchport mode { **access** | **trunk** }

Parameters

access

Sets the Layer 2 interface as access. Access mode assigns the port to a VLAN

trunk

Sets the Layer 2 interface as trunk. Trunk mode makes the port linkable to other switches and routers

Modes

Interface subtype configuration mode

Usage Guidelines

You must configure the same native VLAN on both ends of an 802.1 or classified VLAN trunk link. Failure to do so can cause bridging loops and VLAN leaks.

Examples

To set the mode of a specific 10-gigabit Ethernet interface to *access* :

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode access
```

To set the mode of a specific port-channel interface to trunk:

```
switch(config)# interface port-channel 44
switch(config-port-channel-44)# switchport mode trunk
```

switchport mode private-vlan

Sets the private VLAN (PVLAN) mode of the Layer 2 interface.

Syntax

switchport mode private-vlan [**host**] [**promiscuous**] [**trunk** [**promiscuous** | **host**]]

Command Default

The port does not have any PVLAN attributes by default.

Parameters

host
Sets the port mode to host (community or isolated) mode. It accepts the untagged or priority tagged packet, and the outgoing packet is untagged.

promiscuous
Sets the port mode to promiscuous mode.

trunk
Sets the port mode to PVLAN trunk port. This port can carry multiple VLANs. The outgoing packets carry all VLANs, except for native VLANs.

trunk host
Sets the port mode to host (community or isolated) mode. The trunk operand means the outgoing packet will be tagged "accept".

trunk promiscuous
Sets the trunk to promiscuous mode.

Modes

Interface subtype configuration mode

Usage Guidelines

This command assigns the primary Vlan to a promiscuous port. This command also maps a promiscuous port to selected secondary VLANs. This means only selected VLANs can send packets to this port.

All switchport modes are independent from each other, including normal mode (access/trunk) and above private VLAN modes. Based on the default behavior of the port, the new mode automatically overwrites the existing mode by deleting the existing mode (removing any relationship/association) and applying the new mode.

Examples

To set the mode of a specific 10-gigabit Ethernet interface to PVLAN trunk:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode private-vlan trunk
```

To set the mode of a specific 10-gigabit Ethernet interface to PVLAN promiscuous (untagged):

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode private-vlan promiscuous
```

To set the mode of a specific 10-gigabit Ethernet interface to PVLAN promiscuous (tagged):

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode private-vlan trunk promiscuous
```

switchport mode trunk-no-default-native

Configures a port to trunk mode without the implicit creation of default native VLAN 1 in a Virtual Fabrics context.

Syntax

switchport mode trunk-no-default-native

Modes

Interface subtype configuration mode

Usage Guidelines

When this command is enabled, any ingress tagged or untagged packet is discarded until a switchport classification or native VLAN classification is configured. To disable this functionality, simply issue the **no switchport** command, or enter a different switchport mode by using the **switchport mode access** command or the **switchport mode trunk** command.

Port mode change is not allowed when port security is enabled on the interface.

This is the fundamental difference between this command and the **switch mode trunk** command, which implicitly creates VLAN 1 on the port.

The global command **dot1q tag native-vlan** does not affect the ingress or egress tagging behavior of the native VLAN configured in this mode.

The following native VLAN commands are supported in this mode:

- **switchport trunk native-vlan-untagged**
- **switchport trunk native-vlan-xtagged**

The following native VLAN commands that are supported in regular trunk mode are NOT supported in this mode:

- **switchport trunk tag native-vlan**
- **switchport trunk native-vlan**

Examples

Configure a trunk port without a default native VLAN, then explicitly configure the native VLAN.

```
switch(config)# interface te 2/1/1
switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native
switch(config-if-te-2/1/1)# switchport trunk native-vlan-xtagged 1 egress tagged
```

Related Commands

switchport trunk native-vlan, switchport trunk native-vlan-untagged, switchport trunk native-vlan-xtagged

switchport port-security

Enables or disables port security on an interface port.

Syntax

switchport port-security

no switchport port-security

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no switchport port-security** command to disable port security on the interface.

Port mode change is not allowed when port security is enabled on the interface.

switchport port-security mac-address

Configures the MAC address option for port security on an interface port.

Syntax

switchport port-security mac-address *address* **vlan** *vlan_id*

Parameters

mac-address *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface subtype configuration mode

switchport port-security max

Configures the maximum number of MAC addresses used for port security on an interface port.

Syntax

switchport port-security max *value*

no switchport port-security max

Parameters

value

The maximum number of secure MAC addresses. Range is from 1 through 8192.

Modes

Interface subtype configuration mode

switchport port-security oui

Configures an Organizationally Unique Identifier (OUI) MAC address for port security on an interface port. All other addresses are ignored

Syntax

switchport port-security oui *address*

no switchport port-security oui

Parameters

address

The OUI MAC address from which to accept vendor traffic, in the format xxxx.xxxx.xxxx.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no switchport port-security oui** command to disable this option.

The use of static secure MAC addresses is not included in OUI-based port security.

When you configure the first OUI MAC address on a secure port, traffic floods until the entries are programmed in the hardware.

switchport port-security shutdown-time

Configures the shutdown-time option for port security on an interface port.

Syntax

switchport port-security shutdown-time *time*

Parameters

time

The amount of time to shut down the interface port, in minutes. Range is from 1 through 15.

Modes

Interface subtype configuration mode

switchport port-security sticky

Converts dynamic MAC addresses to sticky secure MAC addresses.

Syntax

switchport port-security sticky mac-address *address* **vlan** *vlan_id*

Parameters

mac-address *address*
Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*
Specifies a VLAN.

Modes

Interface subtype configuration mode

Usage Guidelines

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. When this command is executed on an interface, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

switchport port-security violation

Configures the violation response options for port security on an interface.

Syntax

switchport port-security violation { **restrict** | **shutdown** }

Parameters

restrict

Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.

shutdown

Puts the interface into the error-disabled state for a predetermined amount of time.

Modes

Interface subtype configuration mode

switchport private-vlan association trunk

Assigns a primary private VLAN to private VLAN trunk port.

Syntax

switchport private-vlan association trunk *primary_vlan_ID secondary_vlan_ID*

no switchport private-vlan association trunk *primary_vlan_ID*

no switchport private-vlan association trunk *primary_vlan_ID secondary_vlan_ID*

Command Default

The port does not have any PVLAN attributes by default.

Parameters

primary_vlan_ID
The primary VLAN identification.

secondary_vlan_ID
The secondary VLAN identification.

Modes

Interface subtype configuration mode

Usage Guidelines

Multiple PVLAN pairs (Primary VLAN, multiple secondaries) can be specified using this command. Therefore, two **no** versions of this command are used to remove association for one primary VLAN, or remove any trunk association.

Examples

To associate a primary VLAN to PVLAN trunk port, in this example 2 is primary VLAN and 302 is secondary VLAN:

```
switch(conf-if-te-178/0/9)# switchport private-vlan association trunk 2 302
```

To remove a primary VLAN to PVLAN trunk port:

```
switch(conf-if-te-178/0/9)# no switchport private-vlan association trunk 2
```

Related Commands

private-vlan, switchport mode private-vlan, switchport private-vlan mapping

switchport private-vlan host-association

Assigns a secondary and primary VLAN pair to host port.

Syntax

switchport private-vlan host-association *primary_vlan_ID secondary_vlan_ID*

no switchport private-vlan host-association

Command Default

The port does not have any PVLAN attributes by default.

Parameters

primary_vlan_ID
The primary VLAN identification.

secondary_vlan_ID
The secondary VLAN identification.

Modes

Interface subtype configuration mode

Related Commands

private-vlan, switchport mode private-vlan, switchport private-vlan mapping

switchport private-vlan mapping

Maps primary VLAN and secondary VLAN to a promiscuous port.

Syntax

switchport private-vlan mapping *primary_vlan_ID* [**add** | **remove**] *secondary_vlan*

no switchport private-vlan mapping

Command Default

The port does not have any PVLAN attributes by default.

Parameters

primary_vlan_ID
The primary VLAN identification.

add
Adds the secondary VLAN to the primary mapping.

remove
Removes the secondary VLAN from the primary mapping.

secondary_vlan
The secondary VLAN identification.

Modes

Interface subtype configuration mode

Usage Guidelines

This command also maps a promiscuous port to selected secondary VLANs. This means only selected VLAN can send packets to this port.

Related Commands

private-vlan, switchport private-vlan association trunk

switchport private-vlan trunk allowed vlan

Adds a VLAN to a private VLAN (PVLAN) trunk port.

Syntax

switchport private-vlan trunk allowed vlan { **all** | **none** | [**add** | **remove** | **except**] *vlan_id*] **ctag** *ctag* }

no switchport private-vlan trunk allowed vlan *vlan_id*

Command Default

The port will have default VLAN 1.

Parameters

all
Allows all VLANs.

none
Removes all VLANs except for VLAN 1.

add
Adds a specified VLAN.

remove
Removes the specified VLAN.

except
Allows all VLANs except the specified VLAN.

vlan_id
Specifies a VLAN.

ctag *ctag*
Specifies an incoming C-TAG that is associated with a service or transport VF in a Virtual Fabrics context.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to remove a VLAN or C-TAG from a trunk port.

For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, and FCoE VLAN, or an internal control VLAN.Examples

The following illustrates the configuration of PVLANs for both 802.1Q VLANs and service or transport VFs in a Virtual Fabrics context.

Configure a PVLAN trunk port:

```
switch(config)# int te 4/1
switch(config-if-te-2/0/2)# switchport mode private-vlan trunk
```

Configure 802.1Q VLANs and service or transport VFs in a Virtual Fabrics context:

```
switch(config-if-te-2/0/2)# switchport private-vlan trunk allowed vlan add 400
switch(config-if-te-2/0/2)# switchport private-vlan trunk allowed vlan add 5000 ctag 100
```

Configure service or transport VFs as PVLANs, by using the **switchport private-vlan association** command:

```
switch(config-if-te-2/0/2)# switchport private-vlan association trunk 6000 7000
switch(config-if-te-2/0/2)# switchport private-vlan association trunk 6000 8000
```

Related Commands

switchport mode, switchport private-vlan association trunk

switchport private-vlan trunk native-vlan

Sets native private VLAN (PVLAN) characteristics of the Layer 2 trunk interface for classifying untagged traffic.

Syntax

switchport private-vlan trunk native-vlan *vlan_id*

no switchport private-vlan trunk native-vlan

Parameters

vlan_id

Specifies a VLAN to transmit and receive through the Layer 2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no switchport trunk native-vlan** to reset the native VLAN to the default setting.

Native VLAN configuration is not supported for a port in private vlan trunk promiscuous mode.

Examples

To set native PVLAN characteristics for a VLAN whose VLAN ID is 120:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport private-vlan trunk native-vlan 120
```

Related Commands

switchport mode private-vlan, switchport private-vlan association trunk, switchport private-vlan trunk allowed vlan

switchport trunk allowed vlan rspan-vlan

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Syntax

switchport trunk allowed { **vlan** | **rspan-vlan** } { **add** *vlan_id* { **ctag** { *id* | *ctag* **-** *range* } | **all** | **except** *vlan_id* | **none** | **remove** *vlan_id* }

Parameters

add *vlan_id*
: Adds a VLAN to transmit and receive through the Layer 2 interface. The VLAN can be an 802.1Q VLAN, an RSPAN VLAN, or a transport VLAN.

all
: Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to classified or transport VLANs.

ctag
: Specifies an incoming C-TAG or range of C-TAGs for classified or transport VLANs in a Virtual Fabrics context.

id
: C-TAG ID.

range
: Range of C-TAG IDs, for example, 100-200, or 10,20,100-200, applicable only if the VLAN is a transport VLAN.

except *vlan_id*
: Allows only 802.1Q VLANs except the specified VLAN ID to transmit and receive through the Layer 2 interface.

none
: Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to service or transport VFs in a Virtual Fabrics context.

rspan-vlan *vlan_id*
: Selects a VLAN for Remote Switched Port Analyzer (RSPAN) traffic monitoring.

remove *vlan_id*
: Removes a VLAN that transmits and receives through the Layer 2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, and FCoE VLAN, or an internal control VLAN.

A transport VF C-TAG can be any VLAN ID that is not used in other classifications or as a 802.1Q VLAN.

Examples

To add the tagged VLAN 100 to a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk allowed vlan add 100
```

To remove the tagged VLAN 100 from the interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk allowed vlan remove 100
```

The following examples illustrate configuration in a Virtual Fabrics context:

Configure an interface as a trunk switchport.

```
switch(config)# int te 1/0/1
switch(config-if-te-1/0/1)# switchport mode trunk
```

A C-TAG is required for a classified VLAN (VLAN ID from 4096 through 8191):

```
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 7000
switch(config-if-te-1/0/1)# syntax error: unknown argument
```

Configure a classified VLAN with a C-TAG:

```
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 5000 ctag 100
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 6000 ctag 200
```

An 802.1Q vlan specified as a user VLAN cannot be used as a C-TAG in a classified VLAN. The following show conflicts.

- Edge C-TAG 100 is already assigned to VLAN 5000 at the same port:

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 8000 ctag 100
switch(config-if-te-1/0/1)# %Error: C-tag is already used.
```

- Edge VLAN 100 is already used as a C-TAG in a classified VLAN:

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan 100
switch(config-if-te-1/0/1)# %%Error: One of the vlans in the range is configured as a ctag on the same
port.
switch(config-if-te-1/0/1)# switchport trunk allow vlan all
switch(config-if-te-1/0/1)# %%Error: Virtual-fabric vlan classification configuration exists.
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 888
```

- Edge VLAN 888 was already used in 802.1Q configuration.

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 8000 ctag 888
switch(config-if-te-1/0/1)# %Error: Ctag is configured in the allowed range on this port.
```

switchport trunk default-vlan

Configures tagged or untagged data traffic that does not match any classification rule on a trunk port, supporting service or transport VFs in a Virtual Fabrics context.

Syntax

switchport trunk default-vlan *vlan_id*

no switchport trunk default-vlan *vlan_id*

Parameters

vlan_id

Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

Enter **no switchport trunk default-vlan** *vlan_id* to remove the default VLAN configuration.

Examples

Create a transport VF in a Virtual Fabrics context:

```
switch(config)# interface vlan 6000
switch(config-vlan-6000)# transport-service 60
```

Classify all nonmatching traffic except native VLAN traffic to the transparent default VLAN:

```
switch(config-if-te-2/0/1)# switchport trunk default-vlan 6000
```

switchport trunk native-vlan

Sets native VLAN characteristics as an 802.1Q VLAN, or, in a Virtual Fabrics context, as service or transport VF on a trunk port, matching tagged or untagged data traffic that does not match a classification rule.

Syntax

switchport trunk native-vlan *vlan_id* [**ctag** *id*]

no switchport trunk native-vlan *vlan_id* [**ctag** *id*]

Parameters

vlan_id

Adds a VLAN to transmit and receive through the Layer 2 interface.

ctag *id*

Sets an optional C-TAG for a service or transport VF (VLAN ID > 4095). If not present, the native VLAN is untagged.

Modes

Interface subtype configuration mode

Usage Guidelines

Note the following:

- For VLAN IDs above 4095, the **ctag** keyword is optional.
- If **ctag** is not used, the native VLAN is untagged and the command is validated against the **[no] switchport trunk tag native-vlan** command, which controls the tagging of the native VLAN at the interface level. The **switchport trunk native-vlan** command is accepted only if the configuration set by the **switchport trunk tag native-vlan** command allows untagged packets. For VLAN IDs above 4095, validation against the global command **no vlan dot1q tag native** is not required.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- For 802.1Q VLANs (VLAN ID < 4096), both the interface subtype and global commands that control native VLAN tagging apply to the specified native VLAN.

Use the **no** form of this command to unconfigure the native VLAN. VLAN 1 then becomes the native VLAN.

For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, or an internal control VLAN. An FCoE VLAN ID can be used as a C-TAG provided the interface is not configured for "fcoeport default."

Enter **no switchport trunk native-vlan** to reset the native VLAN to the default setting

Examples

To set native VLAN characteristics for an 802.1Q VLAN whose VLAN ID is 120:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk native-vlan 120
```

The following illustrates the use of the command in a Virtual Fabrics context:

- Configure an interface as a switchport trunk and set the tagging of the native VLAN at the interface level:

```
switch(config)# int te 2/0/1
switch(config-if-te-2/0/1)# switchport mode trunk
switch(config-if-te-2/0/1)# switchport trunk tag native-vlan
```

- Change the native VLAN from the default of 1 to a classified VLAN (VLAN ID > 4095) and add an optional C-TAG:

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000 ctag 50
```

- Change the new native default VLAN to an 802.1Q VLAN (VLAN ID < 4096):

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 200
```

- The interface must allow untagged packets for classified native VLANs without a C-TAG:

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000
%%Error: Cannot configure non-dot1q native-vlan without a ctag, when native-vlan-tagging is enabled.
switch(config-if-te-2/0/1)# no
 switchport trunk tag native-vlan
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000
```

switchport trunk native-vlan-untagged

Configures a port to accept only untagged packets, and specifies that those packets be egress untagged in a Virtual Fabrics context. The untagged packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.

Syntax

switchport trunk native-vlan-untagged *vlan_id*

no switchport trunk native-vlan-untagged

Parameters

vlan_id

Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Use the **no switchport trunk native-vlan-untagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure untagged native VLAN 5000, allow VLAN 6000, and make VLAN 7000 the default VLAN.

```
switch(config)# interface te 2/1/1
switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native
switch(config-if-te-2/1/1)# switchport trunk native-vlan untagged 5000
switch(config-if-te-2/1/1)# switchport trunk add vlan 6000 ctag 100-200
switch(config-if-te-2/1/1)# switchport trunk default-vlan 7000
```

Remove the native VLAN 5000.

```
switch(config-if-te-2/1/1)# no switchport trunk native-vlan-untagged
```

Related Commands

switchport mode trunk-no-default-native, switchport trunk native-vlan-xtagged

switchport trunk native-vlan-xtagged

Configures a port to accept both tagged and untagged packets, and specifies the egress tagging behavior in a Virtual Fabrics context.

Syntax

switchport trunk native-vlan-xtagged *vlan_id* [**ctag** *cvid*] **egress** { **tagged** | **untagged** | **any** }

no switchport trunk native-vlan-xtagged

Parameters

vlan_id
: Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

ctag *cvid*
: Sets an optional C-TAG (802.1Q VLAN ID) for a service or transport VF (VLAN ID > 4095).

egress
: Enables the selection of required tagging options.

  tagged
  : Specifies packets as tagged.

  untagged
  : Specifies packets as untagged.

  any
  : Specifies that packets preserve their ingress encapsulation.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Note the following:

- Ingress packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- If the specified VLAN is an 802.1Q VLAN, the **ctag** option is not required.
- If the specified VLAN is an 802.1Q VLAN or a service VF, the **egress** tagging options are **tagged** or **untagged**.
- If the specified VLAN is a transport VF, then the **egress** tagging option must be **any** to preserve the encapsulation of ingress frames.

Use the **no switchport trunk native-vlan-xtagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure transport VF 6000 that accepts C-TAG range 100 through 200 and a native VLAN that can be either tagged or untagged.

```
switch(config)# interface te 2/1/1
switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native
switch(config-if-te-2/1/1)# switchport trunk native-vlan-xtagged 6000 ctag 10 egress any
switch(config-if-te-2/1/1)# switchport trunk allow vlan 6000 ctag 100-200
```

Remove the native VLAN from the transport VF.

```
switch(config-if-te-2/1/1)# no switchport trunk native-vlan-xtagged
```

Related Commands

switchport mode trunk-no-default-native, switchport trunk native-vlan-untagged

switchport trunk tag native-vlan

Enables tagging on native VLAN traffic.

Syntax

switchport trunk tag native-vlan

no switchport trunk tag native

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no switchport trunk tag native** to untag native traffic for a specific interface.

Examples

To enable tagging for native traffic on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport trunk tag native-vlan
```

system-description

Sets the global system description specific to LLDP.

Syntax

system-description *line*

no system-description

Parameters

line

Specifies a description for the LLDP system. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-description** to clear the global LLDP system description.

Examples

To set the global system description specific to LLDP:

```
switch(conf-lldp)# system-description Brocade
```

Related Commands

system-name

system-max

Sets the maximum number of Address Resolution Protocol (ARP) requests that the system will allocate.

Syntax

system-max arp *number_of_arps*

no system-max arp

Parameters

arp

Enables setting the maximum number of ARP requests.

number_of_arps

An integer value from 0 through 16384.

Modes

RBridge ID configuration mode

Usage Guidelines

Use the **no** form of this command to disable this feature.

system-monitor

Manages the monitoring of FRUs and sets a variety of alerts when thresholds are exceeded.

Syntax

system-monitor { **LineCard** [**alert** [**action** [**all** | **email** | **none** | **raslog**]] | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] | **MM** [**threshold** [**down-threshold** | **marginal-threshold**]] | **cid-card** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] | **compact-flash** [**threshold** [**down-threshold** | **marginal-threshold**]] | **fan** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] | **power** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] **sfp** [**alert** [**action state**]] **temp** [**threshold** [**down-threshold** | **marginal-threshold**]] }

no system-monitor

Command Default

For system monitoring defaults, see the "System Monitor" chapter in the *Network OS Administrator's Guide Supporting Network OS v.4.0.0* .

Parameters

LineCard
Specifies alerts and thresholds for line cards.

MM
Specifies thresholds for management modules.

cid-card
Specifies alerts and thresholds for the chassis ID card.

compact-flash
Specifies thresholds for the compact flash device.

fan
Specifies alerts and thresholds for the fans.

power
Specifies alerts and thresholds for the power supplys.

sfp
Specifies alerts for the small form-factor pluggable devices.

temp
Specifies thresholds for the temperature sensors.

alert
Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

action
Specifies the response type.

all
Specifies that e-mail and RASLog messaging are used.

email
Specifies that an e-mail message is sent.

none
Specifies that no message is sent.

raslog
Specifies RASLog messaging.

state
Specifies the hardware state to be monitored.

all
Specifies that all hardware states are monitored.

faulty
Specifies that hardware is monitored for faults.

inserted
Specifies that the insertion state of hardware is monitored.

none
Specifies that no hardware states are monitored.

on
Specifies that the hardware on/off state is monitored.

removed
Specifies that the removal of hardware is monitored.

threshold
Specifies the monitoring of thresholds

down-threshold
Specifies an integer value that, when exceeded, indicates when hardware is down.

marginal-threshold
Specifies an integer value that, when exceeded, indicates when hardware is operating marginally.

Modes

RBridge ID configuration mode

Usage Guidelines

Use this command to configure field-replaceable unit (FRU) monitoring and actions. Depending on these configuration settings, a variety of actions are generated when there is a change in FRU state.

Use this command in RBridge subconfiguration mode to manage the system health monitoring of individual nodes in a cluster.

Examples

```
switch(config-rbridge-id-154)# system-monitor sfm threshold down-threshold 3 marginal-threshold 2
switch(config-rbridge-id-154)# system-monitor cid-card alert state faultyinserted action email
```

Related Commands

rbridge-id, show system monitor, system-monitor-mail

system-monitor-mail

Configures Fabric Watch e-mail alerts on the switch.

Syntax

system-monitor-mail { **fru** | **interface** | **relay** { *host_ip* | *domain_name* } | **security** | **sfp** } **enable** | *email-id*]

no system-monitor-mail

Command Default

The default source is disabled.

Parameters

fru
Configures e-mail alerts for FRUs.

interface
Configures e-mail alerts for interfaces.

relay
Configures the relay host for e-mail to work in a non-DNS environment.

host_ip
Specifies the IPv4 address of the mail server.

domain_name
Specifies the domain that corresponds to the e-mail ID.

security
Configures e-mail alerts for security.

sfp
Configures e-mail alerts for SFPs.

enable
Enables or disables e-mail alerts for the above options.

email-id
Specifies the e-mail address to where the alert will be sent.

Modes

Global configuration mode

Usage Guidelines

For an e-mail alert to function correctly, add the IP addresses and host names to DNS in addition to configuring the domain name and name servers. Both relay parameters (the host IP address and the domain name) must be configured in a non-DNS environment. In a DNS environment, only the host IP address is required).

Examples

```
switch(config)# system-monitor-mail ?

Possible completions:
  fru         Configure FRU mail settings
  interface   Configure interface mail settings
  relay       Configure relay ip mail settings
  security    Configure security mail settings
  sfp         Configure sfp mail settings
switch(config)# system-monitor-mail fru enable

switch(config)# system-monitor-mail relay ?

Possible completions:
  <host-ip:IP address>  <host-ip:string, min: 1 chars, max: 253 chars>
switch(config)# system-monitor-mail relay 1.2.3.4 ?

Possible completions:
  domain-name   Domain name server
switch(config)# system-monitor-mail relay 1.2.3.4 domain-name ?

Possible completions:
  <LINE:0-64>   Domain name[]
switch(config)# system-monitor-mail relay 1.2.3.4 domain-name  abc.brocade.com

switch# show running-config system-monitor-mail relay

system-monitor-mail relay 1.2.3.4 domain-name abc.brocade.com
```

To create a mapping:

```
switch(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name abc.brocade.com
```

To delete the mapping:

```
switch(config)# no system-monitor-mail relay host-ip 1.2.3.4
```

To change the domain name:

```
switch(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name mail.brocade.com
```

Related Commands

show system monitor, system-monitor

system-name

Sets the global system name specific to LLDP.

Syntax

system-name *name*

no system-name

Command Default

The host name from the switch is used.

Parameters

name

Specifies a system name for the LLDP. The string must be between 1 and 32 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-name** to delete the name.

Examples

To specify a system name for the LLDP:

```
switch(conf-lldp)# system-name Brocade
```

Related Commands

system-description

system tunnel suppress-debounce

Suppresses the debounce-timer functionality for a tunnel.

Syntax

system tunnel suppress-debounce

no system tunnel suppress-debounce

Command Default

There is a one second delay after the underlay network stops before the tunnel stops.

Modes

Global configuration mode

Usage Guidelines

Use the **no system tunnel suppress-debounce** command to remove the suppression of the delay.

The debounce timer is a one second delay after the underlay network stops before the tunnel stops. This command suppresses that one second delay, so the underlay network and tunnel stop simultaneously.

Examples

Typical command execution.

```
device(config)# system tunnel suppress-debounce
device(config)#
```

History

Release version	Command history
5.0.2b	This command was introduced.

table-map

Maps external entry attributes into the routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

Syntax

table-map *string*

no table-map *string*

Command Default

This option is disabled.

Parameters

string

Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of the command to remove the table map.

Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Configurations made by this command apply to all peers.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP4 routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a table map. The table map does not require separate configuration. You can have only one table map.

NOTE

Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

Examples

The following illustrates the execution of the **table-map** command in the context discussed in Usage Guidelines:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# route-map TAG_IP permit 1
device(config-route-map/TAG_IP/permit/1)# match ip address prefix-list p11
device(config-route-map/TAG_IP/permit/1)# set tag 100
device(config-route-map/TAG_IP/permit/1)# exit
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# table-map TAG_IP
```

To remove the table map:

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no table-map TAG_IP
```

History

Release version	Command history
5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

route-map

tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

Syntax

tacacs-server {**host** *hostname* | **source-ip** [*chassis-ip* | *mm-ip*] } [**port** *portnum*] [**protocol** { **chap** | **pap** }] [**key** *shared_secret*] [**encryption-level** *value_level*] [**timeout** *secs*] [**retries** *num*]

no tacacs-server { **host** *hostname* | **source-ip** [*chassis-ip* | *mm-ip*] }

Command Default

Refer to the Parameter section for specific defaults.

Parameters

host hostname
Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

source-ip [*chassis-ip* | *mm-ip*]
Specifies the chassis IP address or MM IP address as the source IP address for TACACS+ authentication and accounting.

port *portnum*
Specifies the authentication port. Valid values range from 0 through 65535. The default is 49.

protocol { *chap* | *pap* }
Specifies the authentication protocol. Options include CHAP and PAP. The default is CHAP.

key *shared_secret*
Specifies the text string that is used as the shared secret between the switch and the TACACS+ server to make the message exchange secure. The key must be between 8 and 40 characters in length. The default key is **sharedsecret** . The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the password in either double quotes or the escape character (\), for example **"secret!key"** or **secret\!key**.

encryption-level *value_level*
Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

timeout *secs*
Specifies the time to wait for the TACACS+ server to respond. The default is 5 seconds.

retries *num*
Specifies the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

Modes

Global configuration mode

Usage Guidelines

If a TACACS+ server with the specified IP address or host name does not exist, it is added to the server list. If the TACACS+ server already exists, this command modifies the configuration. The **key** parameter does not support an empty string.

Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

> NOTE
> Before downgrading to a Network OS version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will throw an error that requests this value be set to **0**.

Before downgrading to a version that doesn't support **tacacs-server source-ip**, you must remove the source-ip configuration using **no tacacs-server source-ip**. Otherwise, the firmware download process throws an error requesting to reset the cipher.

Examples

To configure an IPv4 TACACS+ server:

```
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries 100
switch (config-tacacs-server-10.24.65.6)#
```

To modify an existing TACACS+ server configuration:

```
switch(config)# tacacs-server host 10.24.65.6
switch(config-tacacs-server-10.24.65.6)# key "changedsec"
```

To delete a TACACS+ server:

```
switch(config)# no tacacs-server host 10.24.65.6
switch(config)# exit
switch# show running-config tacacs-server host
switch# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx key changedsec
```

To configure an IPv6 TACACS+ server:

```
switch(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010 protocol chap
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# key "mysecret"
```

Related Commands

radius-server, show running-config radius-server, show running-config tacacs-server

tagged-ieee-bpdu-enabled

Activates IEEE BPDU packets.

Syntax

tagged-ieee-bpdu-enabled

no tagged-ieee-bpdu-enabled

Modes

mode

Usage Guidelines

Enter **no tagged-ieee-bpdu-enabled** to disable this feature.

This command should only be used on edge ports.

ATTENTION
This command should be enabled when the interface is connected to a switch which sends tagged IEEE bpdu packets.

tcp burstrate

Sets the threshold for the burst rate of TCP traffic, and defines the lockout time once that threshold is passed.

Syntax

tcp burstrate *packet* **lockup** *seconds*

no tcp burstrate

Command Default

This feature is disabled.

Parameters

packet

The maximum number of packets allowed over five seconds. Range is from 1 through 100000.

lockup *seconds*

Sets the number of seconds to lock up the port. Range is from 1 through 3000.

Modes

Global configuration mode

Usage Guidelines

To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive numbers are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

This command sets the threshold for the burstrate, and defines the lockout time once that threshold is passed.

telnet

Establishes a Telnet session to a remote networking device.

Syntax

telnet { *IP_address* | *hostname*}

telnet interface port-num { **interface** | **vrf** *vrf-name* } { *IP_address* | *hostname* }

telnet interface<*N*>**gigabitethernet** { *IP_address* | *hostname* | **vrf** *vrf-name* }

telnet interface management { *IP_address* | *hostname* | **vrf** *vrf-name* }

telnet interface ve *vlan-id hostname*

telnet interface vrf *vrf-name*

telnet vrf *vrf-name*

Command Default

The default port is 23.

Parameters

IP_address

The server IP address in either IPv4 or IPv6 format.

hostname

The host name (a string between 1 and 63 ASCII characters in length.

interface

Specifies an interface.

<*N*> **gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter**?** to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

management

Specifies a management interface.

port-number *port*

Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

ve *vlan-id*

Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

vrf *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

ATTENTION
Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management.

To use the **telnet** command on the management VRF, use the **vrf** keyword and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually.

```
switch# telnet vrf mgmt-vrf
```

The following features are not supported:

- Display Telnet sessions
- Ability to terminate hung Telnet sessions

Examples

To establish a Telnet session from a switch to a remote networking device:

```
switch# telnet 10.17.37.157

Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.
Network OS (sw0)
sw0 login:
```

telnet server shutdown

Disables Telnet service on the switch.

Syntax

telnet server shutdown

no telnet server shutdown

Modes

Global configuration mode

RBridge ID configuration mode

Usage Guidelines

Enter **no telnet server shutdown** to enable Telnet service. This command is not distributed across a cluster. The RBridge ID of the node should be used to configure service on individual nodes.

Examples

To shut down Telnet service on a switch:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# telnet server shutdown
```

To enable Telnet service on a switch:

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no telnet server shutdown
```

Related Commands

show running-config telnet server, show telnet server status

telnet server standby enable

Enables the Telnet services on the standby MM.

Syntax

telnet server standby enable

no telnet server standby enable

Command Default

The Telnet services are disabled on the standby MM.

Modes

RBridge ID configuration mode

Usage Guidelines

The **no telnet server standby enable** command disables the Telnet services on the standby MM.

It is mandatory to specify the default-config when converting from Logical Chassis mode to Fabric Cluster mode, or the other way around. After conversion, the SSH and Telnet services on the standby MMs are disabled. This command enables the Telnet services on the standby MM.

Examples

Typical command output:

```
switch(config-rbridge-id-1)# do show running-config rbridge-id | include standby
% No entries found.
switch(config-rbridge-id-1)# telnet server standby enable
switch(config-rbridge-id-1)# do show running-config rbridge-id | include standby
telnet server standby enable
switch(config-rbridge-id-1)#
```

Typical command output:

```
switch(config-rbridge-id-1)# no telnet server standby enable
switch(config-rbridge-id-1)# do show running-config rbridge-id | include standby
% No entries found.
switch(config-rbridge-id-1)#
```

History

Release version	Command history
5.0.1a	This command was introduced.

Related Commands

ssh server standby enable

terminal

Sets terminal parameters for the current session.

Syntax

terminal [**length** *number_of_lines*] [**monitor**] [**timeout** *value*]

no terminal [**length**] [**monitor**] [**timeout**]

Command Default

The default for **length** is 24.

Parameters

length *number_of_lines*
Specifies the number of lines to be displayed. Valid values range from 1 through 512. Specify 0 for infinite length.

monitor
Enables terminal monitoring.

timeout *value*
Specifies the timeout value in minutes. Valid values range from 0 through 136. Specify 0 to disable timeout.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

This command overrides the timeout configuration set by the **line vty exec-timeout** command, but only for the duration of the current session. When the current session ends, the configured values apply for any subsequent sessions.

This command is not available on the standby management module.

Enter **no terminal** (optionally with a specific parameter) to restore the current terminal settings to default.

Examples

To set the display length to 30 lines:

```
switch# terminal length 30
```

To set the timeout length to 60 minutes:

```
switch# terminal timeout 60
```

To restore all settings to default values:

```
switch# no terminal
```

To restore only the timeout setting to its default values:

```
switch# no terminal timeout
```

Related Commands

line vty exec-timeout

threshold-monitor cpu

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor cpu { [**actions** [**none** | **raslog** [{ **limit** *limit_when_reached* | **poll** *polling_interval* | **retry** *number_of_retries*]] }

no threshold-monitor cpu

Parameters

actions

Specifies the action to be taken when a threshold is exceeded.

none

No action is taken.

raslog

Specifies RASLog messaging.

limit

Specifies the baseline CPU usage limit as a percentage of available resources.

limit_when_reached

When the limit set by this parameter is exceeded, a RASLog WARNING message is sent. When the usage returns below the limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent. The default is 70 percent.

poll

Specifies the polling interval in seconds.

polling_interval

The range is from 0 through 3600. The default is 120

retry

Specifies the number of polling retries before desired action is taken.

number_of_retries

Range is from 1 through 100. The default is 3.

Modes

RBridge ID configuration mode

Usage Guidelines

This command sends a RASLog WARNING message when configured thresholds are exceeded.

Examples

```
switch(config-rbridge-id-154)# threshold-monitor cpu actions rasloglimit 50 poll10
```

Related Commands

rbridge-id

threshold-monitor interface

Configures monitoring of port statistics on all external gigabit Ethernet interfaces: 1 GbE, 10 GbE, and 40 GbE.

Syntax

threshold-monitor interface { [**apply** *policy_name* | **pause** | **policy** *policy_name*] **typeEthernet area** [**CRCAlignErrors** [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]] | **IFG** [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]] | **MissingTerminationCharacter** [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]] | **SymbolErrors**] [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] }

no threshold-monitor interface

Parameters

apply

Applies a custom policy that has been created by the policy operand.

pause

Pause monitoring.

policy

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

WORD

Specifies the name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

type Ethernet

Enables gigabit Ethernet interface monitoring.

area

Enables policy configuration.

CRCAlignErrors

The total number of frames received with either a bad Frame Check Sequence (FCS) or an alignment error.

IFG

The minimum-length interframe gap (IFG) between successive frames is violated. The typical minimum IFG is 12 bytes.

MissingTerminationCharacter

The number of frames that terminate in anything other than the Terminate character.

SymbolErrors
The number of words received as an unknown (invalid) symbol. Large symbol errors indicate a bad device, cable, or hardware.

alert
Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above
Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

below
Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

all
Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of highthresh-action only.

email
Specifies that an email message is sent.

fence
Specifies that Port Fencing is applied, which disables the port until further action is taken This is available only for **highthresh-action**.

none
Specifies that no alert notification or other action (Port Fencing) is taken.

raslog
Specifies RASLog messaging.

limit
Specifies the percent of threshold usage, from 0 through 80. The default is 75.

poll
Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

retry
Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

threshold
Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

buffer
An integer value.

high-threshold
An integer value.

low-threshold
An integer value.

timebase
Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

day
Calculates the difference between a current data value and that value a day ago.

hour
Calculates the difference between a current data value and that value an hour ago.

minute
Calculates the difference between a current data value and that value a minute ago.

none
Compares a data value to a threshold boundary level.

Modes

RBridge ID configuration mode

Usage Guidelines

When any monitored error crosses the configured high or low threshold, an alert is generated and a problem port can be taken out of service. Use this command to monitor port statistics on all external gigabit Ethernet interfaces and generate a variety of actions, from alerts through Port Fencing.

Examples

```
switch(config-rbridge-id-154)# threshold-monitor interface policy mypolicy type Ethernet area IFG alert
above highthresh-action fence raslog lowthresh-action email raslog
```

Related Commands

rbridge-id

threshold-monitor memory

Configures monitoring of the memory usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor memory { [**actions** [**none** | **raslog** { **high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries* } | **high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries* }] }

no threshold-monitor memory

Parameters

actions

Specifies the action to be taken when a threshold is exceeded.

none

No action is taken. This is the default.

raslog

Specifies RASLog messaging.

high-limit

Specifies an upper limit for memory usage as a percentage of available memory.

percent

This value must be greater than the value set by **limit** . When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Values range from 0 through 80 percent. The default is 70 percent.

limit

Specifies the baseline memory usage limit as a percentage of available resources.

percent

When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by **limit** , a RASLog INFO message is sent. Values range from 0 through 80 percent. The default is 60 percent.

low-limit

Specifies a lower limit for memory usage as percentage of available memory.

percent

This value must be smaller than the value set by **limit** . When memory usage exceeds or falls below this limit, a RASLog INFO message is sent. The default is 40 percent.

poll

Specifies the polling interval in seconds.

polling_interval

The range is from 0 through 3600. The default is 120

retry

Specifies the number of polling retries before desired action is taken.

number_of_retries
Range is from 1 through 100. The default is 3.

Modes

RBridge ID configuration mode

Examples

```
switch(config-rbridge-id-154)# threshold-monitor memory actions none high-limit 80 low-limit 50 limit
70 retry 2 poll 30
```

Related Commands

rbridge-id

threshold-monitor security

Configures monitoring of security parameters, such as Telnet and login violations.

Syntax

threshold-monitor security { [**apply** *policy_name* | **pause** | **policy** *policy_name*] **area** [**login-violation** [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**]] | **email** | **fence** | **none** | **raslog**]] | **lowthresh-action** [**all** | **email none** | **raslog**]] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**]] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] | **telnet-violation** [**alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**]] | **email** | **fence** | **none** | **raslog**]] | **lowthresh-action** [**all** | **email none** | **raslog**]] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none raslog**]] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]]]] }

no threshold-monitor security

Command Default

For other security monitoring defaults, see the "System Monitor" chapter in the *Network OS Security Configuration Guide*.

Parameters

apply

Applies a custom policy that has been created by the **policy** operand.

policy_name

Name of a custom policy configuration created by the **policy** operand.

pause

Pauses monitoring.

policy

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

policy_name

Name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

area

Enables policy configuration.

login-violation

Enables monitoring of login violations.

alert

Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above

Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

below

Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

all

Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of **highthresh-action** only.

all

Specifies that email and RASLog messaging are used.

email

Specifies that an email message is sent.

fence

Specifies that Port Fencing is applied, which disables the port until further action is taken.

none

No alert is sent

raslog

Specifies RASLog messaging.

limit

Specifies the percent of threshold usage, from 0 through 80. The default is 75.

poll

Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

retry

Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

threshold

Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

buffer

An integer value.

high-threshold

An integer value.

low-threshold

An integer value.

timebase

Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

day

Calculates the difference between a current data value and that value a day ago.

hour

Calculates the difference between a current data value and that value an hour ago.

minute

Calculates the difference between a current data value and that value a minute ago.

none

Compares a data value to a threshold boundary level.

telnet-violation

Enables monitoring of Telnet violations. Operands are as for **login-violation** .

Modes

RBridge ID configuration mode

Examples

Here are examples of typical commands:

```
switch(config-rbridge-id-154)# threshold-monitor security policy mypolicy area telnet-violation
threshold high-threshold 10 buffer 3

switch(config-rbridge-id-154)# threshold-monitor security policy mypolicy area login-violation timebase
hour
```

Related Commands

rbridge-id

threshold-monitor sfp

Configures monitoring of SFP parameters.

Syntax

threshold-monitor sfp { [**apply** *policy_name* | **pause** | **policy** *policy_name*] **type** *SFP_type* **area** *parameters* **alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] }

no threshold-monitor sfp

Command Default

For the default parameter values of the SFP types, refer to the chapter "System Monitor" in *Network OS Administrator's Guide* .

Parameters

apply

Applies a custom policy that has been created by the **policy** operand.

policy_name

Name of a custom policy configuration created by the **policy** operand.

pause

Pause monitoring.

policy

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

policy_name

Name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

type

Specifies the SFP type. Possible completions are as follows:

1GLR

— SFP Type 1GLR

1GSR

— SFP Type 1GSR

10GLR

— SFP Type 10GLR

10GSR

— SFP Type 10GSR

10GUSR

— SFP Type 10GUSR

100GSR

— SFP Type 100GSR

QSFP

— SFP type QSFP

area

Specifies one of the following SFP parameters to be monitored. See Defaults, below.

Current

Measures the current supplied to the SFP transceiver.

RXP

Measures the incoming laser power, in microWatts (µW).

TXP

Measures the outgoing laser power, in µW).

Temperature

Measures the temperature of the SFP, in degrees Celsius.

Voltage

Measures the voltage supplied to the SFP.

alert

Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above

Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

below

Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

all

Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of **highthresh-action** only.

all

Specifies that email and RASLog messaging are used.

email

Specifies that an email message is sent.

none

Specifies that no alert is sent.

raslog

Specifies RASLog messaging.

limit

Specifies the percent of threshold usage, from 0 through 80. The default is 75.

poll

Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

retry

Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

threshold

Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

buffer

An integer value.

high-threshold

An integer value.

low-threshold

An integer value.

timebase

Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

day

Calculates the difference between a current data value and that value a day ago.

hour

Calculates the difference between a current data value and that value an hour ago.

minute

Calculates the difference between a current data value and that value a minute ago.

none

Compares a data value to a threshold boundary level.

Modes

RBridge ID configuration mode

Examples

A typical command might look like this:

```
switch(config)# threshold-monitor sfp custom type QSFP area rxp threshold high-threshold 2000 low-
threshold 1000
```

Related Commands

rbridge-id

timeout fnm

For Access Gateway mode, this sets and displays the fabric name monitoring time-out value (TOV) for Modified Managed Fabric Name Monitoring (M-MFNM) mode.

Command Default

The default is 120 seconds

Parameters

value

A value from 30 to 120 seconds.

Modes

Access Gateway configuration mode

Usage Guidelines

You must be in Access Gateway (AG) configuration mode to use this command. This command to sets the time out value (TOV) for M-MFNM queries of the fabric name to detect whether all N_Ports in a port group are physically connected to the same physical or virtual fabric. M-MFNM is a Port Grouping mode that prevents connections from the AG VDX switch to multiple SANsEntering the **timeout fnm** command without a value displays the current TOV value.

Examples

Set the fabric name monitoring TOV value.

```
sw0(config-rbridge-id-3-ag)# timeout fnm 60
```

Displays the fabric name monitoring TOV value.

```
sw0(config-rbridge-id-3-ag)# timeout fnm
```

timers

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) throttle timers.

Syntax

timers { **lsa-group-pacing** *interval* | **throttle spf** *start hold max* }

Command Default

See Operands for specific defaults.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

throttle spf

Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 60000 milliseconds. The default is 0 milliseconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 5000 milliseconds.

max

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 10000 milliseconds.

Modes

OSPF VRF router configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

Enter the **no timers lsa-group-pacing** to restore the pacing interval to its default value.

Enter **no timers throttle spf** to set the SPF timers back to their defaults.

Examples

To set the LSA group pacing interval to 30 seconds:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

To change the SPF delay to 10000 milliseconds, the hold time to 15000 milliseconds, and the maximum wait time to 30000 milliseconds:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# timers throttle spf 10000 15000 30000
```

timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Syntax

timers { **keep-alive** *keepalive_interval* **hold-time** *holdtime_interval* }

no timers

Command Default

See Parameters.

Parameters

keep-alive

Sets the interval for KEEPALIVE messages.

keepalive_interval

The KEEPALIVE interval in seconds. Range is from 0 through 65535. Default is 60.

hold-time

Sets the interval for HOLDTIME messages.

holdtime_interval

The HOLDTIME interval in seconds. Range is from 0 through 65535. Default is 180.

Modes

BGP configuration mode

Usage Guidelines

The KEEPALIVE and HOLDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

You must enter a value for **keep-alive** before you can enter a value for **hold-time**. Both values must be entered.

Use the **no timers** command to clear the timers.

Examples

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router bgp
device(config-bgp-router)# timers keep-alive 120 hold-time 360
```

Related Commands

fast-external-fallover

timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers { **lsa-group-pacing** *interval* | **spf** *start hold* }

Command Default

Enabled. Refer to the Parameters section for specific defaults.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds. The default is 5 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds. The default is 10 milliseconds.

Modes

OSPFv3 VRF router configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

Enter the **no timers lsa-group-pacing** to restore the pacing interval to its default value.

Enter **no timers spf** to set the SPF timers back to their defaults.

Examples

To set the LSA group pacing interval to 30 seconds:

```
device# configure terminal
device(config)# rbridge-id 122
device(config-rbridge-id-122)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

History

Release version	Command history
5.0.0	This command was introduced.

traceroute

Traces the network path of packets as they are forwarded to a destination address.

Syntax

traceroute *IPv4_address* |*hostname*[**src-addr** *src-addr*] | [**ipv6** *dest-ipv6-addr*] | *host-name* [**maxttl** *value*] [**minttl** *value*] [**timeout** *seconds*] [**vrf** *vrf-name*]

Parameters

IPv4_address
Specifies the IPv4 address of the destination device.

hostname
Specifies the hostname of the destination device.

ipv6 *dest-ipv6-addr*
Specifies the IPv6 address of the destination device. This parameter is valid only with the **ping** command.

maxttl *value*
Maximum Time To Live value in a number of hops.

minttl *value*
Minimum Time To Live value in a number of hops.

src-addr *address*
Specifies the IPv4 or IPv6 address of the source device.

timeout *seconds*
The traceroute timeout value.

vrf *vrf-name*
Name of the VRF. If no VRF is specified, the default-vrf is used. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

ATTENTION
Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management.

To use the **traceroute** command on the management VRF, enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually.

```
switch# traceroute 1.1.1.1 vrf mgmt-vrf
```

Examples

To execute an IPv4 traceroute.

```
switch# traceroute 172.16.4.80

traceroute to 172.16.4.80 (172.16.4.80), 64 hops max
 1   10.24.80.1 (10.24.80.1) 0.588ms 0.139ms 0.527ms
 2   10.31.20.61 (10.31.20.61) 0.550ms 0.254ms 0.234ms
 3   10.16.200.113 (10.16.200.113) 0.408ms 0.285ms 0.282ms
 4   10.110.111.202 (10.110.111.202) 5.649ms 0.283ms 0.288ms
 5   10.130.111.38 (10.130.111.38) 1.108ms 0.712ms 0.704ms
 6   10.192.0.42 (10.192.0.42) 37.053ms 32.985ms 41.744ms
 7   172.16.56.10 (172.16.56.10) 33.110ms 33.349ms 33.114ms
 8   172.16.4.9 (172.16.4.9) 34.096ms 33.023ms 33.122ms
 9   172.16.4.80 (172.16.4.80) 76.702ms 83.293ms 79.570ms
```

To execute an IPv6 traceroute, with minimum and maximum TTL values.

```
switch# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 maxttl 128 minttl 30 src-addr fec0:60:69bc:
92:205:33ff:fe9e:3f20 timeout 3

traceroute to fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470), 128 hops max, 80
byte packets
30  fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470)  2.145 ms  2.118 ms  2.085
ms
```

Related Commands

ping

track

Specifies a VRRP interface to track.

Syntax

track { <*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | } [**priority** *range*]

no track { <*N*>**gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | } [**priority** *range*]

Command Default

Priority range is 2.

Parameters

<*N*>**gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace <*N*>**gigabitethernet** with the desired operand (for example, tengigabitethernet specifies a 10-Gb Ethernet port). The use of gigabitethernet without a speed value specifies a 1-Gb Ethernet port.

rbridge-id

Specifies an RBridge ID.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *number*

Specifies the port-channel number. Valid values range from 1 through 6144.

priority *range*

The track priority is a number from 1 through 254, and is used when the tracked interface up or down event is detected. For VRRP, if the tracked interface becomes disabled, the current router priority is reduced *to* the track-port priority, (For VRRP only, interface tracking does not have any effect on an owner router; the owner priority can not be changed from 255.) For VRRP-E, if the tracked interface becomes disabled, the current router priority is reduced *by* the track-port priority.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command can be used for VRRP or VRRP-E.

For VRRP, the tracked interface can be any 10-gigabit Ethernet, 40-gigabit Ethernet, 1-gigabit Ethernet, or port-channel interface other than the one on which this command is issued.

The maximum number of interfaces you can track per virtual router is 16.

Enter **no track** with the specified interface to remove the tracked port configuration.

Examples

To set the track port to 21/2/4 and the track priority to 60:

```
switch(config)# rbridge-id 21
switch(config-rbridge-id-21)# protocol vrrp
switch(config-rbridge-id-21)# int te 21/1/6
switch(conf-if-te-21/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# track tengigabitethernet 21/2/4 priority 60
```

Related Commands

vrrp-group

track (Fabric-Virtual-Gateway)

Tracks an interface, network, or next hop.

Syntax

track interface {*<N>* **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* } **priority** *range*

no track interface {*<N>* **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* } **priority** *range*

track network *A.B.C.D/mask* **priority** *range*

no track network *A.B.C.D/mask*

track next-hop *ip-address* **priority** *range*

no track next-hop *ip-address*

Command Default

None

Parameters

interface
Interface type.

network
Network address

next-hop
Next hop IP address

*<N>***gigabitethernet**
Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace*<N>***gigabitethernet** with the desired operand (for example, tengigabitethernet specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

rbridge-id
Specifies an RBridge ID.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

port-channel *number*
Specifies the port-channel number. Valid values range from 1 through 6144.

priority *range*
The track priority range is from 1 through 254.

A.B.C.D/mask
Network address in A.B.C.D/mask format.

ip-address
IP address.

Modes

Fabric-virtual-gateway in an RBridge VE interface IPv4 or IPv6 configuration mode

Usage Guidelines

Enter the **no** form of the command with the specified interface to remove the tracked port configuration.

Examples

The following example shows how to track a fortygigabitethernet interface with a priority of 34.

```
sw0(config)# rbridge-id 55
sw0(config-rbridge-id-55)# interface ve 1
sw0(config-Ve-1)# ip fabric-virtual-gateway
sw0(config-ip-fabric-virtual-gw)# track interface fortygigabitethernet 55/0/51 priority 34
```

The following example shows how to track a network with a priority of 28.

```
sw0(config)# rbridge-id 58
sw0(config-rbridge-id-58)# interface ve 1
sw0(config-Ve-1)# ipv6 fabric-virtual-gateway
sw0(config-ipv6-fabric-virtual-gw)# track network 1::1/22 priority 28
```

History

Release version	Command history
5.0.1	This command was introduced.

transmit-holdcount

Configures the maximum number of Bridge Protocol Data Units (BPDUs) transmitted per second for the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), and R-PVST+.

Syntax

transmit-holdcount *number*

no transmit-holdcount

Command Default

6 units

Parameters

number

Specifies the number of BPDUs than can be sent before pausing for 1 second. Valid unit values range from 1 through 10.

Modes

Protocol Spanning Tree MSTP configuration mode

Usage Guidelines

Brocade Network OS supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no transmit-holdcount** to return to the default setting.

Examples

To change the number of BPDUs transmitted to 3 units:

```
switch(conf-mstp)# transmit-holdcount 3
```

Related Commands

show spanning-tree mst detail

transport-service

In a Virtual Fabrics context, associates a service VF with a trunk port interface as a transport VF.

Syntax

transport-service *tlsid*

no transport-service *tlsid*

Command Default

This feature is disabled by default.

Parameters

tlsid

The transport LAN service ID. Range is from 1 through 1000.

Modes

Interface subtype configuration mode

Usage Guidelines

In a Virtual Fabrics context, use this command to associate a service VF (VLAN ID > 4095, through 8191) to a trunk port interface as a transport VF.

This command does not apply to standard (802.1Q) VLANs (VLAN IDs from 1 through 4095).

This command is not supported when issued from a secondary node.

Enter **no transport-service** *tlsid* to remove the service VF from the trunk port interface as a transport VF.

Examples

Configure a classified VLAN and assign it to transport VF instance 10:

```
switch(config)# interface vlan 5000
switch(config-vlan-5000)# transport-service 10
```

Related Commands

interface vlan, vcs virtual-fabric enable

trunk-enable

Enables port trunking on a Fibre Channel port.

Syntax

trunk-enable

no trunk-enable

Modes

Interface Fibre Channel configuration mode

Usage Guidelines

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6740 and VDX 2740 switches), in Brocade VCS Fabric mode.

A long-distance link can also be configured to be part of a trunk group.

While using R_RDY mode flow control, an E_Port cannot form trunk groups of long distance links even if trunking is enabled.

To disable trunking on a Fibre Channel port, enter **no trunk-enable**.

Examples

This example enables trunking mode on a Fibre Channel port:

```
switch(config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# trunk-enable
```

This example disables trunking mode on a Fibre Channel port:

```
switch (config)# interface FibreChannel 7/0/2
switch(conf-FibreChannel-7/0/2)# no trunk-enable
```

type

Specifies whether a VXLAN overlay gateway uses NSX Controller integration or Layer 2 extension.

Syntax

type { **nsx** | **layer2-extension** }

Command Default

NSX Controller integration is the default behavior.

Parameters

nsx
Specifies NSX Controller integration.

layer2-extension
Specifies Layer 2 extension.

Modes

VXLAN overlay gateway configuration mode.

Usage Guidelines

There is no **no** form of this command, as the overlay gateway must have a type.

Note the following restrictions related to changing the type:

- To change the type, ensure that the gateway is not attached to any RBridge.
- If changing from **nsx** to **layer2-extension**, ensure that there are no "attach vlan" configurations, as configured by the **attach vlan** command.
- If changing from **layer2-extension** to **nsx**, ensure that no "map vlan" configurations are present, as configured by the **map vlan** command.

Examples

To specify Layer 2 extension:

```
switch# config
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# type layer2-extension
```

Related Commands

attach vlan, map vlan, overlay-gateway

type (FlexPort)

Sets the FlexPort interface to support either Ethernet or Fibre Channel protocol.

Syntax

type { **fibre-channel** | **ethernet** }

Command Default

The default state is set to Ethernet protocol.

Parameters

fibre-channel

Sets the interface type to Fibre Channel protocol.

ethernet

Sets the interface type to Ethernet protocol.

Modes

FlexPort configuration mode

Examples

To set the FlexPort interface type to Fibre Channel:

```
switch(config)# hardware
switch(config-hw)# flexport 1/0/1
switch(conf-hw-flex-1/0/1)# type fibre-channel
```

To set the FlexPort interface type to Ethernet:

```
switch(config)# hardware
switch(config-hw)# flexport 1/0/1
switch(conf-hw-flex-1/0/1)# type ethernet
```

History

Release version	Command history
5.0.0	This command was introduced.

udld enable

Enables the Unidirectional Link Detection (UDLD) protocol on an interface.

Syntax

udld enable

no udld enable

Command Default

Disabled on interfaces by default.

Modes

Interface subconfiguration mode (fo, gi, te)

Usage Guidelines

Use **no udld enable** to unblock the interface if it has been blocked by the UDLD protocol.

Examples

To enable UDLD on a specific tengigabitethernet interface:

```
switch# configure
switch(config)# interface te 5/0/1
switch(conf-if-te-5/0/1)# udld enable
```

Related Commands

protocol udld

unhide built-in-self-test

Executes the built-in self test for Federal Information Processing Standards (FIPS).

Syntax

unhide built-in-self-test

Modes

Privileged EXEC mode

Usage Guidelines

Irreversible commands related to enabling FIPS compliance are hidden. Use this command to execute the built-in self test of the FIPS system.

Enter "fibranne" at the Password prompt to run the command.

This command applies only in fabric cluster mode. This command can be entered only from a user account with the admin role assigned.

Examples

To execute the built-in self test for FIPS:

```
switch# unhide built-in-self-test
Password: ********
```

History

Release version	Command history
5.0.1	This command was introduced.

unhide fips

Makes available irreversible commands used in enabling Federal Information Processing Standard (FIPS) compliance.

Syntax

unhide fips

Modes

Privileged EXEC mode

Usage Guidelines

Irreversible commands related to enabling FIPS compliance are hidden. Use this command to make the following hidden commands available: **fips root disable**, **fips selftests**, **fips selftests**, and **prom-access disable**.

Enter "fibranne" at the Password prompt to run the command.

This command applies only in fabric cluster mode. This command can be entered only from a user account with the admin role assigned.

Examples

To make available all irreversible commands used in enabling FIP compliance:

```
switch# unhide fips

Password: *****
```

unlock username

Unlocks a locked user account.

Syntax

unlock username *name* [**rbridge-id** { *rbridge-id* | **all** }]

Parameters

name

The name of the user account.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to unlock a user who has been locked out because of unsuccessful login attempts. A user account is locked by the system when the configured threshold for login retries has been reached.

Examples

The following example unlocks a user account:

```
switch# unlock username testUser
Result: Unlocking the user account is successful
```

Related Commands

show running-config username, show sfp, username

update-time (BGP)

Configures the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

Syntax

update-time *sec*

no update-time *sec*

Command Default

This option is disabled.

Parameters

sec

Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

The update time determines how often the device computes the routes (next-hops) in an RBridge. Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP4 next-hop tables and affected BGP4 routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP4 convergence for situations such as a link failure or IGP route changes, starting the BGP4 route calculation in sub-second time.

Use the **no** form of this command to restore the defaults.

NOTE

Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

Examples

To permit fast convergence:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# update-time 0
```

History

Release version	Command history
NOS v5.0.0	This command was modified to add support for the IPv6 address family.

Related Commands

advertisement interval (fabric-map)

usb

Enables or disables an attached USB device. The device will be inaccessible until it is enabled

Syntax

usb { **on** | **off** }

Parameters

on

Turns the USB device on.

off

Turns the USB device off.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local switch. A switch reload will automatically turn the USB device off.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To enable a USB device attached to the local switch:

```
switch# usb on

USB storage enabled
```

To disable a USB device attached to the local switch:

```
switch# usb off

USB storage disabled
```

Related Commands

usb dir, usb remove

usb dir

Lists the contents of an attached USB device.

Syntax

usb dir

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local switch. The USB device must be enabled before this function is available.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To list the contents of the USB device attached to the local switch:

```
switch# usb dir

firmwarekey\ 0B 2010 Aug 15 15:13
support\ 106MB 2010 Aug 24 05:36
support1034\ 105MB 2010 Aug 23 06:11
config\ 0B 2010 Aug 15 15:13
firmware\ 380MB 2010 Aug 15 15:13
Available space on usbstorage 74%
```

Related Commands

usb, usb remove

usb remove

Removes a file from an attached USB device.

Syntax

usb remove directory *directory* **file** *file*

Parameters

directory *directory*

Specifies one the name of the directory where the file you want to remove is located. Valid USBstorage directories are /firmware, /firmwarekey, /support, and /config.

file *file*

Specifies the name of the file to be removed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local switch. The USB device must be enabled before this function is available.

This command is supported only on the local switch.

This command is not supported on the standby management module.

Examples

To remove a configuration file from a USB device attached to the local switch:

```
switch# usb remove directory config file startup-config.backup
```

Related Commands

usb, usb dir

user (alias configuration)

Launches the user level alias configuration mode.

Syntax

user *string*

no user *string*

Parameters

string

Alias name string. The number of characters can be from 1 through 64.

Modes

Alias configuration mode

Usage Guidelines

The suser alias is only visible to the user currently logged in to the switch. Use the **alias** command to configure the alias for the user name.

Use the **no** form of his command to remove the user

Examples

Example of setting a switch alias and a user alias.

```
switch(config)# alias-config
switch(config-alias-config)# alias redwood engineering
switch(config-alias-config)# user john
switch(config-alias-config-user)# alias johnexpansion smith
switch(config-alias-config-user)# alias userinfo show users
```

Related Commands

alias, alias-config

username

Configures a user account.

Syntax

username *username* **password** *password* **role** *role_name* [**encryption-level** { 0 | 7 }] [**desc** *description*] [**enable true** | **false**]

no username *name*

Command Default

The default account status is enabled (enable = true).

The default role has read-only access permissions.

Parameters

username
Specifies the account login name.

password *password*
Specifies the account password. The exclamation mark (!) is supported, and you can specify the password in either double quotes or the escape character (\), for example "secret!password" or **secret\!password.**

role *role_name*
Specifies the role assigned to the user account. The role is optional and, by default, the user's role is read-only.

encryption-level { 0 | 7 }
Specifies the password encryption level. The values are 0 (clear text) and 7 (encrypted). Clear text (0) is the default.

desc *description*
Specifies a description of the account (optional). The description can be up to 64 characters long, and can include any printable ASCII character, except for the following characters: single quotation marks (‘), double quotation marks (“), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces. you must enclose the text in double quotation marks.

enable true | **false**
Specifies whether the account is enabled or disabled. A user whose account is disabled cannot login. The default account status is enabled.

Modes

Global configuration mode

Usage Guidelines

The *username* must be between 1 and 40 characters in length. The username must begin with a letter or underscore and be comprised of only letters, numbers, underscore and period. The username is case sensitive. The name cannot be the same as that of an existing role.

The maximum number of user accounts on a switch is 64.

The maximum number of roles for a user is 64, including the default roles.

Enter **no username** *name* followed by the appropriate parameter name to set the individual parameters to their default values. Use this command to assign attributes for a user.

CAUTION
All active login sessions for a user are terminated if the user's password or role is changed.

Examples

To configure a user account:

```
switch(config)# username testUser roles admin
Value for 'password' (<string>): **********

switch(config-username-testUser)# exit
switch(config)# username userBrocade password ******** role user desc "User to monitor" enabled true
switch(config-username-userBrocade)#
```

To modify an existing user account:

```
switch(config)# username testUser enabled false
switch(config-username-testUser)# desc "add op test user"
switch(config)# no username testUser desc
```

Related Commands

show running-config username, show users, unlock username

username admin enable false

Toggles the lockout option for the default admin account.

Syntax

username admin enable false

no username admin enable false

Command Default

This feature is disabled.

Modes

Global configuration mode

Usage Guidelines

This command toggles the lockout option for the default admin account.

The account lockout policy locks an account when the user exceeds the configured number of maximum failed login attempts. This policy is now available for admin accounts. You are allowed to enable or disable lockout policy for admin accounts and user accounts with the admin role.

For admin accounts, there is no support of lockout duration to release the locked accounts. Locked admin role accounts will be reset after reboot.

Use the **no** username admin enable false command to disable this option.

username user enable false

Toggles the lockout option for user accounts with admin privileges.

Syntax

username user enable false

no username user enable false

Command Default

This feature is disabled.

Modes

Global configuration mode

Usage Guidelines

This command toggles the enable option for user accounts with admin privileges.

The account lockout policy locks an account when the user exceeds the configured number of maximum failed login attempts. This policy is now available for admin accounts. You are allowed to enable or disable lockout policy for admin accounts and user accounts with 'admin' role.

Use the **no username user enable false** command to disable this option.

use-v2-checksum

Enables the v2 checksum computation method for a VRRPv3 IPv4 session.

Syntax

use-v2-checksum

no use-v2-checksum

Command Default

VRRPv3 uses the v3 checksum computation method.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Some non-Brocade devices only use the v2 checksum computation method in VRRPv3. This command enables v2 checksum computation method in VRRPv3 and provides interoperability with these non-Brocade devices.

The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on a Brocade device.

```
device(config)# rbridge-id 1
device(config-rbridge-id-1)# protocol vrrp
device(config-rbridge-id-1)# interface ve 100
device(config-Ve-100)# vrrp-group 10 version 3
device(config-vrrp-group-10)# use-v2-checksum
```

History

Release version	Command history
5.0.1a	This command was introduced.

vcenter

Authenticates with an established vCenter and provides additional options.

Syntax

vcenter *name* [**activate** | **interval** *interval* | { **url** *URL* **username** *username* **password** *password* }]

no vcenter *name*

Parameters

name
Name of an established vCenter.

activate
Activates the vCenter.

interval
Enables the discovery timer.

interval
Discovery timer interval in minutes, Range is 0 through1440. Default is 30, and 0 disables discovery.

url
Enables configuration of vCenter URL, user name, and password.

URL
URL of the vCenter.

username
Configures the user name.

password
Configures the password.

Modes

Global configuration mode

Usage Guidelines

You must authenticate with an established vCenter before you can initiate any discovery transactions. In order to authenticate with a specific vCenter, you must configure the URL, login, and password properties on the VDX switch. Use this command to authenticate with a vCenter; establish a URL, username, and password; and manage discovery intervals.

Enter **no vcenter** *name* and selected operands to deactivate this functionality.

Examples

```
switch(config)# vcenter myvcenter url https://10.2.2.2 username user password pass
switch(config)# vcenter myvcenter activate
switch(config)# no vcenter myvcenter activate
switch(config)# no vcenter myvcenter
switch(config)# vcenter myvcenter interval 60
```

Related Commands

show vlan private-vlan

vcenter discovery (ignore delete responses)

Causes a vCenter to ignore delete responses.

Syntax

vcenter *name* **discovery ignore-delete-all-response** [*number* | **always**]

Command Default

The default for *number* is 0.

Parameters

name

Name of the vcenter.

number

Number of discovery cycles to ignore. Default is 0.

always

Always ignore delete-all requests from the vCenter.

Modes

Global configuration mode

Usage Guidelines

An invalid state or condition of a vCenter can cause the deletion of all auto-port-profiles in a system. To prevent this from happening, you can configure a mode in Network OS to ignore the "delete-all" responses from the vCenter.

Examples

```
switch(config)# vcenter vcs_demo discovery ignore-delete-all-response 3
```

vc-link-init

Specifies the fill word used on long distance links for an 8 Gbps Fibre Channel port.

Syntax

vc-link-init { **idle** | **arb** }

Command Default

vc-link-init is **idle** .

Parameters

idle

Sets the long distance link fill word to IDLE.

arb

Sets the long distance link fill word to ARB(ff).

Modes

Interface subtype configuration mode

Usage Guidelines

The fill word must be set to the same value as the fill word configured for the remote port. Therefore, if the remote port link initialization and fill word combination is **idle-idle**, then the fill word for the long distance link must be set to **idle**. If the remote port link initialization/fill word combination is set to **arbff-arbff**, **idle-arbff**, or **aa-then-ia** , then the fill word for the long distance link must be set to **arb**.

This command can be used only on Network OS platforms with Fibre Channel ports (Brocade VDX 6740), in Brocade VCS Fabric mode, and with the FCoE license installed.

Examples

To set the fill word for a long distance link:

```
switch (config)# interface FibreChannel 7/0/2

switch(conf-FibreChannel-7/0/2)# vc-link-init arb
```

vcs (logical chassis cluster mode)

Changes the RBridge ID or VCS ID of a logical chassis cluster mode and, with the no form of the command, converts a logical chassis cluster to a fabric cluster.

Syntax

vcs [**rbridge-id** *rbridge-id*] [**vcsid** *vcsid*]

no vcs [**rbridge-id** *rbridge-id*] [**vcsid** *vcsid*] **logical-chassis enable**

no vcs logical-chassis enable rbridge-id { **all** | *range* } **default-config**

Parameters

rbridge-id *rbridge-id*
Changes the existing RBridge ID.

vcsid *vcsid*
Changes the VCS ID. The range for this value is 1 to 8192. The default is 1.

logical-chassis enable
Used with the **no** form of this command, transitions the node from logical chassis cluster mode to fabric cluster mode.

rbridge-id [**all** | *range*]
Specifies that you want to either convert all RBridge IDs in the logical chassis cluster to fabric cluster mode, or that you want to convert only a range of RBridge IDs. (You can also specify just one RBridge ID.) Ranges can be specified with hyphens, separated by commas, or contain a mixture of both. Do not use a space after a comma when specifying a range of IDs. For example, to specify RBridges 5 through 10 and RBridge 15, enter: **rbridge-id 5,10,15**

default-config
Uses the default configuration when the nodes are converted to fabric cluster mode. This is a required parameter.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to change the RBridge ID and/or the VCS ID on a switch. At the same time, you can change the VCS ID and transition the node from logical chassis cluster mode to fabric cluster mode. You can also convert the cluster from logical chassis cluster mode to fabric cluster mode without changing the RBridge ID or VCS ID.

For examples of how to use the **no** form of this command, refer to the Examples.

Examples

To change the RBridge ID to 10 and VCS ID to 35:

```
switch# vcs rbridge-id 10 vcsid 35
```

To change an RBridge ID from 8 to 10:

```
switch# vcs rbridge-id 10
```

During reboot, enter the following command on the principal node to disable the old RBridge ID:

```
switch# no vcs enable rbridge-id 8
```

The following examples illustrate the use of the **no** form of this command.

- Change the RBridge ID of the node to the value <x> and then transitions the node from logical chassis cluster mode to fabric cluster mode.

```
switch# no vcs rbridge-id <x> logical chassis enable
```

- Change the VCS ID of the node to the value <y> and then transitions the node from logical chassis cluster mode to fabric cluster mode.

```
switch# no vcs vcs-id <y> logical chassis enable
```

- Changesthe RBridge ID of the node to the value <x>, changes the VCS ID of the node to the value <y>, and then transitions the node from logical chassis cluster mode to fabric cluster mode.

```
no vcs rbridge-id <x> vcsid <y> logical chassis enable
```

- Convert the entire logical chassis cluster (all RBridge IDs) to fabric cluster mode. The nodes will then use the default configurations for fabric cluster mode.

```
no vcs logical-chassis enable rbridge-id all default-config
```

- Converts RBridge IDs 1 and 4 through 8 from logical chassis cluster mode to fabric cluster mode. These RBridge IDs will then use the default configurations for fabric cluster mode.

```
no vcs logical-chassis enable rbridge-id 1,4-8 default-config
```

vcs config snapshot (logical chassis cluster mode)

Takes a configuration snapshot for a specified RBridge ID.

Syntax

vcs config snapshot { **create** | **restore** } **rbridge-id** *rbridge-id* **snapshot-id** *snapshot-id*

no config snapshot rbridge-id *rbridge-id* **snapshot-id** [**all** | *rbridge-id*]

Parameters

create
Captures the snapshot configuration from the RBridge ID specified.

restore
Restores the snapshot configuration to the RBridge ID specified.

rbridge-id *rbridge-id*
Specifies the RBridge ID of the configuration you are capturing in a snapshot or the RBridge ID to which you are restoring the snapshot.

snapshot-id *snapshot-id*
Name you give to the snapshot of the configuration.

all
Designates all of the snapshots.

Modes

Privileged EXEC mode

Usage Guidelines

A configuration snapshot allows you to restore the configuration if necessary. The snapshot for the RBridge specified is stored on all switches in the logical chassis cluster.

The **vcs config snapshot** commands apply onto to nodes in a logical chassis cluster mode. The **create** and **restore** commands can be issued from any node in the cluster even though the commands pertain to a specific RBridge ID.

If a snapshot was taken on a node that had been disconnected from the cluster, the cluster will not have the snapshot. In this situation, you can use the **copy snapshot** commands to put the snapshot on the cluster.

Examples

To create a snapshot of the configuration on an RBridge with the ID of 10, and to give the name of the snapshot "snapshot10:"

```
switch# vcs config snapshot create rbridge-id 10 snapshot snapshot10
```

vcs logical-chassis enable (fabric cluster mode)

Changes specified nodes from fabric cluster mode to logical chassis cluster mode.

Syntax

vcs logical-chassis enable rbridge-id { **all** | *range* } **default-config**

no vcs logical-chassis enable rbridge-id { **all** | *range* } **default-config**

Parameters

rbridge-id [**all** | *range*]

Specifies that you want to either convert all RBridge IDs in the fabric cluster from fabric cluster mode to logical chassis mode, or that you want to convert only a range of RBridge IDs. (You can also specify just one RBridge ID.) Ranges can be specified with hyphens, separated by commas, or contain a mixture of both. Do not use a space after a comma when specifying a range of IDs. For example, to specify RBridges 5 through 10 and RBridge 15, enter: **rbridge-id 5,10,15**

default-config

Uses the default configuration when the nodes are converted to logical chassis mode. This is a required parameter.

Modes

Privileged EXEC mode

Usage Guidelines

In logical chassis mode, configuration can be distributed from one node—the primary switch—to all other nodes in the cluster.

Each time you change the Brocade VCS Fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you issue any of the commands shown in the Synopsis.

This command can be run only when the switch is in fabric cluster mode. All nodes you want to convert to logical chassis cluster mode must have the same global configuration for this command to work.

Conversely, the **no** form of the command can be run only when the switch is in logical chassis cluster mode and you want to convert it to fabric cluster mode.

Examples

To convert all RBridge IDs in the fabric cluster to logical chassis cluster mode:

```
switch# vcs logical-chassis enable rbridge-id all default-config
```

vcs rbridge-id (fabric cluster mode)

Changes the RBridge ID and, optionally, the VCS ID, and can enable logical chassis cluster mode.

Syntax

vcs rbridge-id *rbridge-id* [**logical-chassis enable** | **vcsid** *vcsid* [**logical-chassis enable**]]

Parameters

rbridge-id *rbridge-id*

Allows you to change the existing RBridge ID, and gives you the option of changing the VCS ID at the same time. While changing these IDs, you can also enable logical chassis cluster mode on the specified RBridge ID.

vcsid *vcsid*

Changes the VCS ID. The range for this value is 1 to 8192. The default is 1.

logical-chassis enable

Enables logical chassis cluster mode on the switch.

Modes

Privileged EXEC mode

Usage Guidelines

Each time you change the Brocade VCS Fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you issue any of the commands shown in the Synopsis.

Examples

To convert a node that is in fabric cluster mode to logical chassis cluster mode, while simultaneously changing its RBridge ID to 10 and its VCS ID to 35:

```
switch# vcs rbridge-id 10 vcsid 35 logical-chassis enable
```

vcs vcsid (fabric cluster mode)

Changes the VCS ID and, optionally, the RBridge ID, and can enable logical chassis cluster mode.

Syntax

vcs vcsid *vcsid* [**logical-chassis enable** | **rbridge-id** *rbridge-id* [**logical-chassis enable**]]

Parameters

vcsid *vcsid*
Changes the existing VCS ID. The range for this value is 1 to 8192. The default is 1.

rbridge-id *rbridge-id*
Changes the existing RBridge ID.

logical-chassis enable
Enables logical chassis cluster mode on the switch.

Modes

Privileged EXEC mode

Usage Guidelines

Each time you change the Brocade VCS Fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you issue any of the commands shown in the Synopsis.

Examples

To convert a node that is in fabric cluster mode to logical chassis cluster mode, while simultaneously changing its RBridge ID to 10 and its VCS ID to 35:

```
switch# vcs vcsid 35 rbridge-id 10 logical-chassis enable
```

vcs virtual-fabric enable

Enables the Virtual Fabrics feature, allowing the configuration of service or transport VFs in a Virtual Fabrics context. This expands the VLAN ID address space above the standard 802.1Q limit of 4095 to support multitenancy.

Syntax

vcs virtual-fabric enable

no vcs virtual-fabric enable

Command Default

This feature is disabled by default.

Modes

Global configuration mode

Usage Guidelines

This command will be successful only if the Virtual Fabric (VF) status is VF-capable. This operation does not disrupt existing 802.1Q traffic in the fabric. Upon the successful completion of the command, the status of the fabric becomes VF-enabled.

Use the **no** form of this command to disable the configuration of service or transport VFs in the fabric. The **no** form of this command will be successfl only if there is no serviceor transport VF configuration in the fabric and the status of the fabric is VF-enabled. All service or transport VF configurations in the fabric must be removed or the command **no vcs virtual-fabric enable** will fail. Upon successful completion of the command, the fabric status becomes VF-capable.

On the Brocade VDX family of switches, VLANs are treated as interfaces from a configuration point of view. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

  NOTE
  When the fabric is VF-enabled with a VF-specific configuration, the user is advised of relevant errors when attempting to disable the VF.

Examples

To enable the Virtual Fabrics feature:

```
switch(config)# vcs virtual-fabric enable
```

To disable the Virtual Fabrics feature when there is no classified VLAN configuration in the fabric:

```
switch(config)# no vcs virtual-fabric enable
```

Related Commands

interface vlan

vcs replace rbridge-id

Replaces a node in a logical chassis cluster.

Syntax

vcs replace rbridge-id *rbridge-id*

Parameters

rbridge-id *rbridge-id*

Specifies the RBridge ID of the node you are replacing.

Modes

Privileged EXEC mode

Usage Guidelines

You most re-use the RBridge ID and then enter the WWN of the new node when prompted, as shown in the Example

This command can be performed only on a node that is in logical chassis cluster mode.

Examples

To replace a node that has an RBridge ID of 3 and then enter the WWN of the new switch:

```
switch# vcs replace rbridge-id 3
Enter the WWN of the new replacement switch: 11:22:33:44:55:66:77:81
```

vcs virtual ip

Assigns a single virtual IP address to all switches in a Brocade VCS Fabric.

Syntax

vcs virtual ip address *ipv4_address/prefix_len*

no vcs virtual-ip address

Parameters

ipaddress

Configures the virtual IP address.

ipv4_address/prefix_len

Specifies the IP address in IPv4 format by means of a CIDR prefix (mask).

Modes

Global configuration mode

Usage Guidelines

When you configure the virtual IP address is configured for the first time, the address is assigned to the principal switch. You can then access the principal switch through the management port IP address or the virtual IP address. The virtual IP configuration is global in nature. All the nodes in the fabric will be configured with the same virtual IP address, but the address is always bound to the current Principal switch

This command can be used in VCS mode only after the fabric has formed successfully.

The command can be executed from any node. However, you cannot remove a virtual IP address when you are logged on to the switch using the virtual IP address. Use the management port IP address or the serial console to configure the virtual IP address.

It is the responsibility of Network Administrator to ensure that the virtual IP address assigned is not a duplicate of address assigned to any other management port in the VCS fabric.

The virtual IP address should be configured on the same subnet as the management interface IP address.

Enter **no vcs virtual ip address** to remove the currently configured virtual IP address.

Examples

To assign a virtual IP address and mask to the principal switch and verify the operation:

```
switch(config)# vcs virtual ip address 10.21.87.2/20

switch(config)# do show vcs virtual ip

Virtual IP              :10.21.87.2/20
Associated rbridge-id   : 2
```

To remove the currently configured virtual IP address:

```
switch(config)# no vcs virtual ip address
```

Related Commands

show vcs

virtual-fabric

Designates the FCoE Virtual Fabric Identification (VFID).

Syntax

virtual-fabric 1

Modes

FCoE fabric-map configuration mode

Usage Guidelines

The VFID value is 1. No other values are allowed.

You must be in the feature configuration mode for FCoE fabric-map for this command to function.

NOTE

The FCoE virtual fabric is not to be confused with the Virtual Fabric feature that supports service or transport VFs.

Examples

```
switch(config)# fcoe

switch(config-fcoe)# fabric-map default

switch(config-fcoe-fabric-map)# virtual-fabric 1
```

virtual-ip

Configures a virtual IPv4 address or IPv6 address for the virtual router.

Syntax

virtual-ip { *ipv4-address* | *ipv6-address* }

no virtual-ip { *ipv4-address* | *ipv6-address* }

Parameters

ipv4-address
Virtual IPv4 address of the virtual router.

ipv6-address
Virtual IPv6 address of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The virtual IPv4 address or IPv6 address is the IP address that an end-host sets as its default gateway. The virtual IP address must belong to the same subnet as the underlying interface. A maximum of 16 virtual IP addresses can be configured for VRRP; only one virtual IP address can be configured for VRRP-E. The session is enabled as soon as the first virtual IP address is configured.

You can perform this command for VRRP or VRRP-E. VRRPv3 introduced the ability to use an IPv6 address when an IPv6 VRRPv3 group is configured.

Enter the **no virtual-ip** command with a specified virtual IP address to delete the specified virtual IP address

Examples

To assign a virtual IP address of 192.53.5.1 to the VRRP virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1
switch(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IP address of 192.53.5.1 to the VRRP-E virtual group 1:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# int ve 20
switch(config-ve-20)# vrrp-group-extended 1
switch(config-vrrp-extended-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IPv6 address of 2001:2019:8192::1 to the VRRP-Ev3 virtual group 19:

```
switch(config)# rbridge-id 122
switch(config-rbridge-id-122)# ipv6 protocol vrrp-extended
switch(config-rbridge-id-122)# interface ve 2019
switch(config-Ve-2019)# ipv6 address 2001:2019:8192::122/64
switch(config-Ve-2019)# ipv6 vrrp-extended-group 19
switch(config-vrrp-extended-group-19)# virtual-ip 2001:2019:8192::1
```

Related Commands

vrrp-group

virtual-mac

Enables generation of a virtual MAC with 0 IP hash.

Syntax

virtual-mac *virtual_mac_address*

Parameters

virtual_mac_address

Modes

VRRP-Extended group configuration mode

Usage Guidelines

The distributed VXLAN gateway functionality depends on VRRP-E for multi-homing. By default, the VRRP-E virtual MAC is derived as 02:e0:52:*<2-byte-ip-hash>* :*<1-byte-vrid>* . The VXLAN gateway requires that the virtual MAC be a function of only VRID. The two-byte hash of the virtual IP should be set to zeros, for example, 02e0.5200.00xx:*<1-byte-VRID>.*

Examples

To enable the generation of a virtual MAC with 0 IP hash:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 10
switch(config-Ve-10)# vrrp-extended-group 100
switch(config-vrrp-extended-group-100)# virtual-mac 02e0.5200.00xx:<1-byte-VRID>
```

vlag ignore-split

Controls the ignore-split recovery functionality.

Syntax

vlag ignore-split

no vlag ignore-split

Command Default

vlag ignore-split is enabled.

Modes

Port-channel configuration mode

Usage Guidelines

When ignore-spilt-recovery is active, neither of the RBridges modify their actor SID when splitting or rejoining the vLAG. They both advertise VSID and keep both sides of the vLAG alive.

This command is supported only when the switch is operating in Brocade VCS Fabric mode.

Enter **no vlag ignore-split** to disable this functionality.

NOTE
It is recommended that this command be enabled.

Examples

```
switch(config)# interface port-channel 27

switch(config-port-channel-27)# vlag ignore-split
```

vlan classifier activate group

Activates a VLAN classifier group.

Syntax

vlan classifier activate group *number* **vlan** *vlan_id*

no vlan classifier activate group *number*

Parameters

number

Specifies which VLAN classifier group to activate. Valid values range from 1 through 16.

vlan *vlan_id*

Specifies which VLAN interface to activate.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no vlan classifier activate group** *number* to remove the specified group.

Examples

To activate VLAN classifier group 1 for VLAN 5 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/1
switch(conf-if-te-178/0/1)# vlan classifier activate group 1 vlan 5
```

To remove VLAN classifier group 10 from a specific port-channel interface:

```
switch(config)# interface port-channel 44
switch(config-port-channel-44)# no vlan classifier activate group 10
```

Related Commands

interface, vlan classifier group

vlan classifier group

Adds and deletes rules to a VLAN classifier group.

Syntax

vlan classifier group *number* [**add rule** *number* | **delete rule** *number*]

Parameters

number
Specifies the VLAN group number for which rules are to be added or deleted. Valid values range from 1 through 16.

add rule *number*
Specifies a rule is to be added. Valid values range from 1 through 256.

delete rule *number*
Specifies a rule is to be deleted. Valid values range from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

Make sure your converged mode interface is not configured to classify untagged packets to the same VLAN as the incoming VLAN-tagged packets. By configuring a converged interface to classify untagged packets (by using classifiers or the default port *vlan_id*) to the same VLAN as VLAN-tagged packets coming into the interface, the FCoE hardware sends out untagged packets to the CNA. These packets may be dropped, disrupting communications.

Examples

To add rule 1 to VLAN classifier group 1:

```
switch(config)# vlan classifier group 1 add rule 1
```

vlan classifier rule

Creates a VLAN classifier rule to dynamically classify Ethernet packets on an untagged interface into VLANs.

Syntax

vlan classifier rule *rule_id* [[**mac** *mac_address*] | [**proto** { *hex_addr* **encap** { **ethv2** | **nosnapllc** | **snapllc** } | **arp encap** { **ethv2** | **nosnapllc** | **snapllc** } | **ip encap** { **ethv2** | **nosnapllc** | **snapllc** } | **ipv6 encap** { **ethv2** | **nosnapllc** | **snapllc** }]]

no vlan classifier rule

Parameters

rule_id
Specifies the VLAN identification rule. Valid values range from 1 through 2556.

mac
Specifies the Media Access Control (MAC) list.

mac_address
Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

proto
Specifies the protocol to use for the VLAN classifier rule.

hex_addr
An Ethernet hexadecimal value. Valid values range from 0x0000 through 0xffff

arp
Specifies to use the Address Resolution Protocol.

ip
Specifies to use the Internet Protocol.

ipv6
Specifies to use the Internet Protocol version 6.

encap
Specifies to encapsulate the Ethernet frames sent for the VLAN classifier rule.

ethv2
Specifies to use the Ethernet version 2 encapsulated frames.

nosnapllc
Specifies to use the Ethernet version 2 non-SNA frames.

snapllc
Specifies to use the Ethernet version 2 with SNA frames.

Modes

Global configuration mode

Usage Guidelines

VLAN classifiers are created individually and are managed separately. Up to 256 VLAN classifiers can be provisioned. One or more VLAN classifiers can be grouped into a classifier group. This classifier group can further be applied on an interface.

Enter **no vlan classifier rule** *rule_id* to delete the specified rule.

Examples

To create an ARP VLAN classifier rule:

```
switch(config)# vlan classifier rule 2 proto arp encap ethv2
```

Related Commands

show vlan

vlan dot1q tag native

Enables 802.1tagging on the native VLAN on all trunked ports on the switch.

Syntax

vlan dot1q tag native

no vlan dot1q tag native

Command Default

The native VLAN is enabled.

Modes

Global configuration mode

Usage Guidelines

Usually, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The switch will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.

Enter **no vlan dot1q tag native** to disable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch.

Related Commands

switchport mode, switchport trunk allowed vlan rspan-vlan

vlan-profile (AMPP)

Activates the VLAN profile mode for AMPP.

Syntax

vlan-profile

no vlan-profile

Modes

Port-profile configuration mode

Usage Guidelines

The VLAN profile mode for AMPP allows configuration of VLAN attributes of a port-profile.

Enter **no vlan-profile** to delete the profile.

Examples

To create a basic VLAN profile supporting 802.1Q VLANs:

```
switch(config)# port-profile my_profile
switch(conf-port-profile-my_profile)# vlan-profile
```

The following illustrates the creation of port-profiles and vlan-profiles with switchport configurations illustrating VLAN classifications in a Virtual Fabrics context:

```
switch(config)# port-profile pp100
switch(config-port-profile-pp100)# vlan-profile
switch(config-vlan-profile)# switchport
switch(config-vlan-profile)# switchport access vlan 5001 mac 1.1.1
switch(config-vlan-profile)# switchport access vlan 5002 mac 1.1.2
switch(config-vlan-profile)# switchport access vlan 5001 mac-group 11
switch(config-vlan-profile)# port-profile pp101
switch(config-port-profile-pp101)# vlan-profile
switch(config-vlan-profile)# switchport
switch(config-vlan-profile)# switchport mode trunk
switch(config-vlan-profile)# switchport trunk allowed vlan add 5004 ctag 11
switch(config-vlan-profile)# switchport trunk allowed vlan add 5005 ctag 12
switch(config-vlan-profile)# switchport trunk native-vlan 5006 ctag 13
```

vnetwork reconcile vcenter

Synchronizes the device configuration with the configuration discovered by vCenter.

Syntax

vnetwork reconcile vcenter *vCenter_name*

Command Default

The vNetwork information is reconciled.

Parameters

vcenter*vcenter_name*
Specifies a vCenter.

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show vnetwork diff vcenter** command to discover if there are any configuration discrepancies between the current device and the data center. If there are, run the **vnetwork reconcile vcenter** command to correct the discrepancies.

Examples

This example shows that the profiles are not listed in the running-config.

```
device# show vnetwork diff vcenter wpgdc1vcenter
port-profiles not created on Switch
-----------------------------------
auto_wpgdc1vcenter_datacenter-2_128_Network
auto_wpgdc1vcenter_datacenter-2_192_Network-vlan660
auto_wpgdc1vcenter_datacenter-2_64_Network-vlan661

device# vnetwork reconcile vcenter wpgdc1vcenter
!
device#
```

History

Release version	Command history
5.0.2b	This command was introduced.

vnetwork vcenter discover

Explicitly starts the discovery process on the vCenter.

Syntax

vnetwork vcenter *vcenter_name* **discover**

Parameters

vcenter_name
Name of a vCenter.

Modes

Privileged EXEC mode

Usage Guidelines

The discovery of virtual assets from the vCenter occurs during one of the following circumstances:

- When a switch boots up.
- When a new vCenter is configured on the VDX switch and activated (activation turns on the timer processing, set to 180-second intervals.)

When the discovery is explicitly initiated with the CLI.

vrf

Creates and enters Virtual Routing and Forwarding (VRF) configuration mode.

Syntax

vrf *name*

Parameters

name

Character string for the name of the VRF. The string can be up 24 characters long, but should not contain punctuation or special characters.

Modes

RBridge ID configuration mode

vrf forwarding

Configures a management port as a management VRF port.

Syntax

vrf forwarding *mgmt_name*

no vrf forwarding *mgmt_name*

Parameters

mgmt_name
The name of the VRF option for the management port.

Command Default

By default, the out-of-band (OOB) management port (the eth0 interface) is part of the management VRF.

Modes

Interface subtype configuration mode

Usage Guidelines

The "no" form of this command disables the management VRF.

ATTENTION
Support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management. This feature is allowed only on management VRF ports.

The management VRF is a dedicated, secure VRF instance that allows users to manage the router inband on switched virtual interfaces (SVIs) and physical interfaces. The name of this VRF instance is "mgmt-vrf;" this instance cannot be deleted.

A management port is any port that is part of the management VRF. The OOB port cannot be removed from the management VRF. In addition, Layer 3 virtual and physical ports (also known as front-end or inband ports) can be part of the management VRF. Inband ports can be moved, by means of the CLI, into and out of the management VRF.

Examples

To enable the management VRF on an Ethernet interface and assign the interface to a subnet:

```
switch(config)# int te 3/0/2
switch(conf-if-te-3/0/2)# vrf forwarding mgmt-vrf
switch(conf-if-te-3/0/2)# ip addr 10.1.1.1/24
```

To disable a management VRF previously configured on a VE interface:

```
switch(config)# int ve 100
switch(conf-Ve-100)# no vrf forwarding mgmt-vrf
```

History

Release version	Command history
5.0.0	This command was introduced.

vrf-lite-capability

Disables the down-bit (DN bit) that is set when routes are redistributed from multiprotocol BGP (MP-BGP) to OSPF.

Syntax

vrf-lite-capability

no vrf-lite-capability

Modes

OSPF VRF router configuration mode

Usage Guidelines

A customer edge (CE) router acts the provider edge (PE) router in VRF Lite. Because PE routers advertise VPN routes to CE routers with the DN-bit set, these checks should be disabled in a VRF Lite context. If CE routers receive routes with the DN-bit set, they discard those routes.

Enter **no vrf-lite-capability** to disable this feature.

Examples

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf vrf orange
switch(config-router-ospf-vrf-orange)# vrf-lite-capability
```

vrf mgmt-vrf

Configures routes on a management VRF port.

Syntax

vrf mgmt-vrf

no vrf mgmt-vrf

Command Default

None

Modes

RBridge ID configuration mode

Usage Guidelines

The **no** form of this command disables the management VRF.

> ATTENTION
> Beginning with release 5.0.0, support is provided for the management VRF. The default VRF and other user-configured (nondefault) VRFs can no longer be used for router management. This feature is allowed only on management VRF ports.

The management VRF is a dedicated, secure VRF instance that allows users to manage the router inband on switched virtual interfaces (SVIs) and physical interfaces. The name of this VRF instance is "mgmt-vrf;" this instance cannot be deleted.

A management port is any port that is part of the management VRF. The OOB port cannot be removed from the management VRF. In addition, Layer 3 virtual and physical ports (also known as front-end or inband ports) can be part of the management VRF. Inband ports can be moved, by means of the CLI, into and out of the management VRF.

Examples

The following configures an IPv4 route subnet for the management VRF, enters address family IPv4 configuration mode, and assigns the management VRF to an Ethernet interface.

```
switch(config)# rbridge-id 3
switch(confif-rbridge-id-3)# vrf mgmt-vrf
switch(config-vrf-mgmt-vrf)# ip route 10.1.1.0/32 te 3/0/10
```

History

Release version	Command history
5.0.0	This command was introduced.

vrrp-extended-group

Configures a virtual-router-extended group and enters into the virtual router configuration mode..

Syntax

vrrp-extended-group *group-ID*

no vrrp-extended-group *group-ID*

Parameters

group-ID

A user-assigned number from 1 through 128 that you assign to the virtual router group.

Modes

Virtual Ethernet (ve) interface configuration mode

Usage Guidelines

This configuration is for virtual Ethernet (ve) interfaces only.

Enter **no vrrp-extended-group** *group-ID* to remove the specific VRRP Extended group.

If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

Examples

The following example shows how to assign the ve interface with a vlan number of 20 to the virtual router extended group with the ID of 1. (First you must enable VRRP-E on the switch.)

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp-extended
switch(config-rbridge-id-101)# int ve 20
switch(config-ve-20)# vrrp-extended-group 1
```

Related Commands

interface, interface ve, virtual-ip

vrrp-group

Configures a virtual router group (VRRP) and enters into the virtual router configuration mode.

Syntax

vrrp-group *group-ID* [**version** { **2** | **3** }]

no vrrp-group *group-ID* [**version** { **2** | **3** }]

Command Default

VRRP version 2 is the default.

Parameters

group-ID

A value from 1 through 128 that you assign to the virtual router group.

version

Specifies in which version of VRRP the IPv4 VRRP group is to be configured.

2 | **3**

Version 2 or version 3 of VRRP.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no vrrp-group** *group-ID* to remove a specific VRRP group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure. You must disable the VRRP session before using the **no** form of this command.

You can specify in which version of VRRP the VRRP group is configured using the **version** keyword and either 2 or 3 as the version number. VRRPv3 supports both IPv4 and IPv6 addresses.

Examples

The following example shows how to assign the 10-gigabit Ethernet interface 101/1/6 to the virtual router group with the ID of 1. (First you must enable VRRP on the switch.)

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# interface tengigabitethernet 101/1/6
switch(config-if-te-101/1/6)# vrrp-group 1
```

The following example shows how to assign the 10-gigabit Ethernet interface 101/1/6 to the virtual router group with the ID of 1 for VRRPv3. (First you must enable VRRP on the switch.)

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# protocol vrrp
switch(config-rbridge-id-101)# interface te 101/1/6
switch(conf-if-te-101/1/6)# vrrp-group 1 version 3
```

Related Commands

interface

write erase

Returns switch to factory default state.

Syntax

write erase [**RbridgeID** *rbridge-ID*] [**vcs-id** *vcs_id*] [**vcs-mode** {0 | 1 }]

Command Default

None

Parameters

Rbridge ID *rbridge-id*

After reboot, the switch is set to the specified RBridge ID

vcs-id *vcs_id*

After reboot, the switch is set to the specified VCS ID.

vcs-mode

Specifies the mode for the switch after it reboots.

0

The switch comes back up in fabric cluster mode.

1

The switch comes back up in logical chassis cluster mode.

Modes

Privileged EXEC mode

Usage Guidelines

The command can be run only on the active MM. Both MMs will be brought to the specified factory default state, with the following guidelines:

- If you do not specify any optional parameters, this command resets all user configurations, including the management IP address and license.
- If you specify any optional parameters, this command resets all user configurations except the management IP address and license and the parameters that you specified.

This command can be used for switch recovery or switch configuration reset to the factory default state. Due to its disruptive nature, this command prompts the user about the consequence of losing all current user configuration and resetting the switch to the factory default state. It waits for the user's confirmation before proceeding.

Examples

To reset the switch to factory defaults, and to bring the switch back up in logical chassis cluster mode, and with an RBridge ID of 25:

```
switch# writer erase rbridgeid 25 vcs-mode 1
```

History

Release version	Command history
5.0.0	This command was introduced.

zoning defined-configuration alias

Creates or deletes a zone alias, adds one or more members to a zone alias, or removes a member from a zone alias.

Syntax

zoning defined-configuration alias *aliasName*

member-entry *member* [**;** *member*] **...**

no member-entry *member*

no zoning defined-configuration alias *aliasName*

Parameters

alias *aliasName*

Specifies a zone alias.

member-entry *member*

Specifies the WWN of the device to be added to the zone alias.

Modes

Global configuration mode

Zoning configuration mode

Usage Guidelines

This command enters a subconfiguration mode, where you can specify the names of the zone alias members to be added to the defined configuration or removed from the defined configuration.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

Enter the **member-entry** command with one or more specified members n the subconfiguration mode to add one or more members to a zone alias. You specify the zone alias member by its WWN. When adding multiple members in a single command line, the members are added sequentially until all members are added or the first error is encountered.

Enter **no member-entry** *member* to remove a member from a zone alias. You can remove only one member entry each time you enter **no member-entry**.

If you remove the last member from a zone alias and subsequently commit the configuration, the commit operation deletes the zone alias.

Enter **no zoning defined-configuration alias** *aliasName* to delete a zone alias.

The **zoning defined-configuration alias** command changes the defined configuration.

To save the configuration persistently, enter **zoning enabled-configuration cfg-action cfg-save** . For the change to become effective, enable the configuration by entering **zoning enabled-configuration cfgName.**

Examples

To create a zone alias with one member:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:00:01
```

To add two additional WWNs to the zone alias:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:00:02;10:00:00:00:00:00:00:03
```

To remove a WWN from a zone alias:

```
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# no member-entry 10:00:00:00:00:00:00:01
```

To delete a zone alias from the defined configuration:

```
switch(config)# no zoning defined-configuration alias alias1
```

Related Commands

show running-config zoning defined-configuration

zoning defined-configuration cfg

Creates a new zone configuration or adds a zone to an existing configuration.

Syntax

zoning defined-configuration cfg *cfgName*

member-zone *zoneName* [*;zoneName*] **...**

no member-zone *zoneName*

no zoning defined-configuration cfg *cfgName*

Parameters

cfgName
Specifies the name of the zone configuration.

member-zone *zoneName*
Specifies the name of a zone to be added to the configuration or removed from the configuration.

Modes

Global configuration mode

Zoning configuration mode

Usage Guidelines

This command enters a subconfiguration mode where you can specify the names of the member zones to be added to the configuration or removed from the configuration.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

The **zoning defined-configuration cfg** command changes the defined configuration. To save the configuration persistently, issue the **zoning enabled-configuration cfg-action cfg-save** command. For the change to become effective, enable the configuration with the **zoning enabled-configuration cfg-name** command.

Enter the **member-zone** command with one or more zone names in the subconfiguration mode to add additional zones. When adding multiple zones in a single command line, the zones are added sequentially until all zones are added or the first error is encountered.

Enter the **no member-zone** with a specified zone name in the subconfiguration mode to remove a member zone from the configuration. You can remove only one member zone each time you enter the **no member-zone** command.

If you enable a zone configuration, the members in that zone configuration must be populated with at least one zone member-entry (a WWN or an alias); otherwise the enable operation fails.

If you remove the last zone from the configuration and subsequently commit the configuration, the commit operation deletes the configuration.

Enter **no zoning defined-configuration cfg** *cfgName* to delete a configuration.

NOTE
Zone aliases are not valid zone configuration members. Adding an alias to an existing zone configuration will not be blocked. However, the attempt to enable a zone configuration that contains aliases will fail with an appropriate error message.

Examples

To add two zones to a zone configuration:

```
switch(config)# zoning defined-configuration cfg cfg4
switch(config-cfg-cfg4)# member-zone zone2;zone3
```

To delete a zone from a zone configuration:

```
switch(config)# zoning defined-configuration cfg cfg4
switch(config-cfg-cfg4)# no member-zone zone2
```

To delete a zone configuration:

```
switch(config)# no zoning defined-configuration cfg cfg4
```

Related Commands

zoning defined-configuration zone, zoning enabled-configuration cfg-name

zoning defined-configuration zone

Creates a new zone or adds a member to an existing zone.

Syntax

zoning defined-configuration zone *zoneName*

member-entry *member* [*; member*] **...**

no member-entry *member*

no zoning defined-configuration zone *zoneName*

Parameters

zone *zoneName*

Specifies the name of the zone to be configured.

member-entry *member*

Specifies the name of the zone member to be added to the zone. The zone member can be specified by a WWN or a by a zone alias.

Modes

Global configuration mode

Zoning configuration mode

Usage Guidelines

Use this command to create a new zone, to add one or more members to a zone, or to delete a member from a zone.

This command enters a subconfiguration mode, where you can specify the names of the zone members to be added to the defined configuration or removed from the defined configuration.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

You can define a zone member by its port WWN or node WWN. However, when creating an LSAN zone, you should use only port WWNs, because node WWNs cannot be exported to a remote fabric.

Enter the **member-entry** command with one or more zone member names in the subconfiguration mode to add additional members to a zone. You can specify the zone member by its WWN or by a zone alias. When adding multiple members in a single command line, the members are added sequentially until all members are added or the first error is encountered.

Enter **no member-entry** *member* to remove a member from a zone. You can remove only one member entry each time you enter **no member-entry**.

If you enable a zone configuration, the members in that zone configuration must be populated with at least one member-entry; otherwise the enable operation fails. However, You can have a non-populated zone in a zone configuration if that zone configuration only exists in the defined-configuration and is not enabled.

If you remove the last member from a zone and subsequently commit the configuration, the commit operation deletes the zone.

Enter **no zoning defined-configuration zone** *zoneName* to delete a zone.

The **zoning defined-configuration zone** command changes the defined configuration:

- To save the configuration persistently, issue the **zoning enabled-configuration cfg-action cfg-save** command.

CAUTION
For the change to become effective, enable the configuration with the zoning enabled-configuration cfg-name command. When edits are made to the defined configuration, and those edits affect a currently enabled zone configuration, issuing a "cfg-save" command makes the enabled configuration effectively stale. Until the enabled configuration is re-enabled, the merging of new RBridges into the cluster is not recommended. This merging may cause unpredictable results, with the potential for mismatched enabled-zoning configurations among the RBridges in the cluster.

Examples

To add a WWN and an alias to a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# member-entry 11:22:33:44:55:66:77:84;alias1
```

To remove a WWN from a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# no member-entry 11:22:33:44:55:66:77:82
```

To remove an alias from a zone:

```
switch(config)# zoning defined-configuration zone zone3
switch(config-zone-zone3)# no member-entry alias1
```

To delete a zone from the defined configuration:

```
switch(config)# no zoning defined-configuration zone zone3
```

Related Commands

zoning defined-configuration cfg

zoning enabled-configuration cfg-action cfg-clear

Clears all zone configurations in the defined configuration.

Syntax

zoning enabled-configuration cfg-action cfg-clear

Modes

Global configuration mode

Usage Guidelines

The enabled configuration is not affected by this command.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

After clearing the defined zone configuration with **zoning enabled-configuration cfg-action cfg-clear**, enter **no zoning enabled-configuration cfg-name** to clear the entire zoning configuration (both the defined zone configuration and the enabled configuration).

If no current active zoning configuration exists, or you just want to clear the defined zone configuration, enter **zoning enabled-configuration cfg-action cfg-save** to commit the transaction.

If a **cfg-clear** is entered accidentally, issue a **cfg-transaction-abort** command.

CAUTION
All defined zone objects in the defined zone configuration are deleted. If you try to commit the empty defined zone configuration while a zone configuration is enabled, you are warned to first disable the enabled zone configuration or to provide a valid configuration with the same name.

Examples

To clear the defined zoning database:

```
switch(config)# zoning enabled-configuration cfg-action cfg-clear
```

Related Commands

zoning enabled-configuration cfg-action cfg-save, zoning enabled-configuration cfg-namezoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-save

zoning enabled-configuration cfg-action cfg-save

Saves the defined configuration to persist across reboots.

Syntax

zoning enabled-configuration cfg-action cfg-save

Modes

Global configuration mode

Usage Guidelines

This command writes the defined configuration and the name of the defined zone configuration to nonvolatile memory in all switches in the VCS Fabric.

The saved configuration is automatically reloaded at power on. If a configuration was in effect at the time it was saved, the same configuration is reinstalled with an automatic **zoning enabled-configuration cfg-name** command.

The **zoning enabled-configuration cfg-action cfg-save** command validates the effective configuration by performing the same tests as the **zoning enabled-configuration cfg-name** command on enabling the configuration. If the tests fail, an error message is displayed and the configuration is not saved.

This command commits the current transaction. Pending transactions are pushed to nonvolatile memory. Any empty zones or empty configurations are deleted.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

Examples

The following example saves the current zone configuration:

```
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

Related Commands

zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-transaction-abort

zoning enabled-configuration cfg-action cfg-transaction-abort

Aborts a current fabric-wide transaction without committing the transaction.

All changes made since the transaction was started are removed and the zone configuration database is restored to the state before the transaction was started.

Syntax

zoning enabled-configuration cfg-action cfg-transaction-abort

Modes

Global configuration mode

Usage Guidelines

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

Examples

To abort the current zone transaction:

```
switch(config)# zoning enabled-configuration cfg-action cfg-transaction-abort
```

Related Commands

zoning enabled-configuration cfg-action cfg-save, zoning enabled-configuration cfg-namezoning enabled-configuration cfg-action cfg-save, zoning enabled-configuration cfg-name

zoning enabled-configuration cfg-name

Enables a zone configuration.

This command commits the current defined zone configuration to both volatile and nonvolatile memory.

Syntax

zoning enabled-configuration cfg-name *cfgName*

no zoning enabled-configuration cfg-name

Command Default

Zoning is not implemented and default zoning applies.

Parameters

cfgName
Specifies the configuration to be enabled.

Modes

Global configuration mode

Usage Guidelines

Only one configuration can be enabled at a time.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

If the operation fails, the previous state is preserved; that is, zoning remains disabled, or the previous effective configuration remains in effect. If the operation succeeds, the new configuration replaces the previous effective configuration.

Enter **no zoning enabled-configuration cfg-name** to disable the currently enabled configuration. The VCS Fabric returns to default zoning mode. In this mode, either all devices can access one another, or no device can access any other device, depending on if the default zoning mode is ALLACCESS or NOACCESS.

NOTE
If more than 300 devices are connected when the enabled-configuration is disabled, the **no zoning enabled-configuration cfg-name** command is not allowed if the defzone mode is AllAccess. In this case, change the defzone mode to No Access and then disable the enabled-configuration.

Examples

To enable a zone configuration:

```
switch(config)# zoning enabled-configuration cfg-name myconfig
```

To disable the currently enabled configuration:

```
switch(config)# no zoning enabled-configuration cfg-name
```

Related Commands

show running-config zoning defined-configuration, show running-config zoning enabled-configuration, zoning enabled-configuration cfg-action cfg-transaction-abort

zoning enabled-configuration default-zone-access

Sets the default zone access mode.

Syntax

zoning enabled-configuration default-zone-access { **allaccess** | **noaccess** }

Command Default

Zone access mode is "All Access".

Parameters

allaccess

Sets the default zone access mode to "All Access". Each device can access all other devices attached to the VCS Fabric.

noaccess

Sets the default zone access mode to "No Access". No device can access any other device in the VCS Fabric.

Modes

Global configuration mode

Usage Guidelines

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all RBridges in the VCS Fabric.

This command can be entered on any RBridge in a Brocade VCS Fabric, but it is always executed on the principal RBridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal RBridge.

ATTENTION

Setting the default zone mode initializes a zoning transaction (if one is not already in progress), and creates reserved zoning objects. For the change to become effective, you must commit the transaction with either the **zoning enabled-configuration cfg-action cfg-save** command or the **zoning enabled-configuration cfg-name** command.

NOTE

A default zone controls the device access that is in effect when zoning is not enabled. When a user-specified zoning configuration is not enabled, the default zone is in effect, allowing access to all devices or no devices. When a user-specified zone configuration is enabled, it overrides the default zone access mode.

Examples

To set the default zone mode to All Access:

```
switch(config)# zoning enabled-configuration default-zone-access allaccess
```

Related Commands

zoning enabled-configuration cfg-name, zoning enabled-configuration cfg-action cfg-save