53-1003389-04
22 January 2016

FastIron

Command Reference

Supporting FastIron Software Release 08.0.20c

BROCADE

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 and modifiers
	Identifies paths and Internet addresses
	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.

Convention	Description
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.
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

What's new in this document

This document is a revision to the first release of the FastIron Command Reference.

In this initial release of the FastIron command reference, not all commands supported on the FastIron devices are represented. All new commands supported in the FastIron Release 08.0.20 and later releases are included.

For new commands introduced since Release 08.0.01, the history table is shown. For legacy commands the history table is not shown unless an update has been added in recent releases.

The following sections list the updates to FastIron Release 08.0.20c.

Modified commands

The following command has been modified.

- mac-auth password-format on page 208

Deprecated commands

The following command has been deprecated.

- **authentication voice-timeout-action**

Supported hardware and software

This guide supports the following product families for FastIron release 08.0.20:

- FCX Series
- FastIron X Series (FSX 800 and FSX 1600)
- ICX 6610 Series
- ICX 6430 Series (ICX 6430, ICX 6430-C12)
- ICX 6450 Series (ICX 6450, ICX 6450-C12-PD)
- ICX 6650 Series
- ICX 7750 Series
- ICX 7450 Series

NOTE
The Brocade ICX 6430-C switch supports the same feature set as the Brocade ICX 6430 switch unless otherwise noted.

NOTE
The Brocade ICX 6450-C12-PD switch supports the same feature set as the Brocade ICX 6450 switch unless otherwise noted.

For information about the specific models and modules supported in a product family, refer to the hardware installation guide for that product family.

Using the FastIron command-line interface

Accessing the CLI

Once an IP address is assigned to a Brocade device running Layer 2 software or to an interface on the Brocade device running Layer 3 software, you can access the CLI either through a direct serial connection or through a local or remote Telnet session.

You can initiate a local Telnet or SNMP or SSH connection by attaching a cable to a port and specifying the assigned management station IP address.

Command modes

The FastIron CLI uses an industry-standard hierarchical shell familiar to Ethernet/IP networking administrators. You can use one of three major command modes to enter commands and access sub-configuration modes on the device.

User EXEC mode

User EXEC mode is the default mode for the device; it supports the lowest level of user permissions. In this mode, you can execute basic commands such as **ping** and **traceroute**, but only a subset of clear, show, and debug commands can be entered in this mode. The following example shows the User EXEC prompt after login. The **enable** command enters privileged EXEC mode.

```
device> enable
device#
```

Privileged EXEC mode

Privileged EXEC mode supports all clear, show, and debug commands. In addition, you can enter some configuration commands that do not make changes to the system configuration. The following example shows the privileged EXEC prompt. At this prompt, you issue the **configure terminal** command to enter global configuration mode.

```
device# configure terminal
device(config)#
```

Global configuration mode

Global configuration mode supports commands that can change the device configuration. For any changes to be persistent, you must save the system configuration before rebooting the device. The global configuration mode provides access to sub-configuration modes for individual interfaces, VLANs,

routing protocols, and other configuration areas. The following example shows how you access the interface sub-configuration mode by issuing the **interface** command with a specified interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)#
```

Command help

You can display commands and syntax information in any mode and from any point in the command hierarchy.

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

```
device(config)#?
  aaa                         Define authentication method list
  access-list                 Define Access Control List (ACL)
  aggregated-vlan             Support for larger Ethernet frames up to 1536 bytes
  alias                       Configure alias or display configured alias
  all-client                  Restrict all remote management to a host
  arp                         Enter a static IP ARP entry
  arp-internal-priority       Set packet priority
  arp-subnet-only             Only learn ARP in the subnet of this device
  authentication              Configure flexible authentication
  banner                      Define a login banner
  batch                       Define a group of commands
  boot                        Set system boot options
  (output truncated)
```

To display a list of commands that start with a specified character, type the character followed by a question mark (?) or a tab.

```
device(config)#e ?
ICX6450-48P Switch(config)#e
  enable                      Password, page-mode and other options
  end                         End Configuration level and go to Privileged level
  errdisable                  Set Error Disable Attributions
  exit                        Exit current level
  extern-config-file          Extern configuration file
```

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

```
deviceh(config)#qos ?
  egress-buffer-profile   User defined QoS egress profile
  mechanism               Change mechanism
  name                    Change name
  profile                 Change bandwidth allocation
  scheduler-profile       User defined QoS profile
  tagged-priority         Change tagged frame priority to profile mapping
```

Command completion

Command completion allows you to execute a command by entering a partial string.

NOTE
Command completion is not supported in the boot loader prompt of ICX 6430 and the ICX 6450 devices.

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. For

example, entering **conf t** in privileged EXEC mode auto-completes the keyword and executes the **configure terminal** as shown.

```
device#conf t
  terminal   Configure thru terminal
deviceh#conf terminal
device(config)#
```

If there is more than one command or keyword associated with the characters typed, the CLI displays all choices matching the characters. Type another character to identify the keyword you are looking for.

```
device(config)#show li
  license                 Show software license information
  link-error-disable      Link Debouncing Control
  link-keepalive          Link Layer Keepalive
device(config)#show lic
  license                 Show software license information
device(config)#show license
```

If you enter an invalid command or partial string that cannot be completed, an error message is displayed.

```
device(config)#shw
Unrecognized command
device(config)#shw
```

Scroll control

By default, the CLI uses a page mode to paginate displays that are longer than 24 lines to 24-line page increments.

If you use the question mark (?) to display a listing of available in a given mode, the display stops at each 24-line increment and lists your choices for continuing the display.

```
aaa
all-client
appletalk
arp
boot
some lines omitted for brevity...

ipx
lock-address
logging
mac
--More--, next page: Space, next line:
Return key, quit: Control-c
```

Use one of the following scrolling options to display additional information:

- Press the **Space bar** to display the next page (one screen at a time).
- Press the **Return** or **Enter** key to display the next line (one line at a time).
- Press **Ctrl+C** or **Ctrl+Q** to cancel the display.
- Use ths **skip** command in privileged EXEC mode to disable page display mode. Use the **page** command to re-enable page display mode

The following example toggles between page display modes.

```
Brocade#skip
Disable page display mode
Brocade#page
Enable page display mode
```

Line editing commands

The CLI supports the following line editing commands. To enter a line-editing command, use the CTRL +key combination for the command by pressing and holding the CTRL key, then pressing the letter associated with the command.

TABLE 1 CLI line editing commands

Ctrl+Key combination	Description
Ctrl+A	Moves to the first character on the command line.
Ctrl+B	Moves the cursor back one character.
Ctrl+C	Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Moves to the end of the current command line.
Ctrl+F	Moves the cursor forward one character.
Ctrl+K	Deletes all characters from the cursor to the end of the command line.
Ctrl+L; Ctrl+R	Repeats the current command line on a new line.
Ctrl+N	Enters the next command line in the history buffer.
Ctrl+P	Enters the previous command line in the history buffer.
Ctrl+U; Ctrl+X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word you typed.
Ctrl+Z	Moves from any CONFIG level of the CLI to the Privileged EXEC level; at the Privileged EXEC level, moves to the User EXEC level.

Searching and filtering command output

You can filter the output from **show** commands at the --More-- prompt. You can search for characters strings, or you can construct complex regular expressions to filter the output.

Searching and filtering output at the --More-- prompt

The --More-- prompt displays when output extends beyond a single page. At this prompt, you can press the Space bar to display the next page, the Return or Enter key to display the next line, or Ctrl +C or Q to cancel the display. In addition, you can search and filter output from this prompt.

At the --More-- prompt, enter a forward slash (/) followed by a search string. The Brocade device displays output starting from the first line that contains the search string as shown in the following example. The search feature is similar to the **begin** option for **show** commands.

```
--More--, next page: Space, next line: Return key, quit: Control-c
/telnet
```

The results of the search are displayed.

```
searching...
  telnet              Telnet by name or IP address
  temperature         temperature sensor commands
  terminal            display syslog
  traceroute          TraceRoute to IP node
  undebug             Disable debugging functions (see also 'debug')
  undelete            Undelete flash card files
  whois               WHOIS lookup
  write               Write running configuration to flash or terminal
```

To display lines containing only a specified search string (similar) press the plus key (+) at the --More-- prompt followed by a search string. This option is similar to the **include** option supported with **show** commands.

```
--More--, next page: Space, next line: Return key, quit: Control-c
+telnet
```

The filtered results are displayed.

```
filtering...
  telnet              Telnet by name or IP address
```

To display lines that do not contain a specified search string, press the minus key (-) at the --More-- prompt followed by a search string. This option is similar to the **exclude** option supported with **show** commands.

```
--More--, next page: Space, next line: Return key, quit: Control-c
-telnet
```

The filtered results are displayed.

```
filtering...
  temperature         temperature sensor commands
  terminal            display syslog
  traceroute          TraceRoute to IP node
  undebug             Disable debugging functions (see also 'debug')
  undelete            Undelete flash card files
  whois               WHOIS lookup
  write               Write running configuration to flash or terminal
```

As with the commands for filtering output from **show** commands, the search string is a regular expression consisting of a single character or string of characters. You can use special characters to construct complex regular expressions. See the next section for information on special characters used with regular expressions.

Searching and filtering show command output

You can filter output from **show** commands to display lines containing a specified string, lines that do not contain a specified string, or output starting with a line containing a specified string. The search string is a regular expression consisting of a single character or a string of characters. You can use special characters to construct complex regular expressions.

Using special characters to construct complex regular expressions

Special characters allow you to construct complex regular expressions to filter output from **show** commands. You can use a regular expression to specify a single character or multiple characters as a search string. In addition, you can include special characters that influence the way the software matches the output against the search string. Supported special characters are listed in the following table.

TABLE 2 Special characters for regular expressions

Character	Operation
.	The period matches on any single character, including a blank space. For example, the following regular expression matches "aaz", "abz", "acz", and so on, but not just "az": a.z
*	The asterisk matches on zero or more sequential instances of a pattern. For example, the following regular expression matches output that contains the string "abc", followed by zero or more Xs: abcX*
+	The plus sign matches on one or more sequential instances of a pattern. For example, the following regular expression matches output that contains "de", followed by a sequence of "g"s, such as "deg", "degg", "deggg", and so on: deg+
?	The question mark matches on zero occurrences or one occurrence of a pattern. For example, the following regular expression matches output that contains "dg" or "deg": de?g **NOTE** Normally when you type a question mark, the CLI lists the commands or options at that CLI level that begin with the character or string you entered. However, if you enter Ctrl+V and then type a question mark, the question mark is inserted into the command line, allowing you to use it as part of a regular expression.
^	A caret (when not used within brackets) matches on the beginning of an input string. For example, the following regular expression matches output that begins with "deg": ^deg
$	A dollar sign matches on the end of an input string. For example, the following regular expression matches output that ends with "deg": deg$

TABLE 2 Special characters for regular expressions (Continued)

Character	Operation
_	An underscore matches on one or more of the following: • , (comma) • { (left curly brace) • } (right curly brace) • ((left parenthesis) •) (right parenthesis) • The beginning of the input string • The end of the input string • A blank space For example, the following regular expression matches on "100" but not on "1002", "2100", and so on. _100_
[ ]	Square brackets enclose a range of single-character patterns. For example, the following regular expression matches output that contains "1", "2", "3", "4", or "5": [1-5] You can use the following expression symbols within the brackets. These symbols are allowed only inside the brackets. • ^ - The caret matches on any characters except the ones in the brackets. For example, the following regular expression matches output that does not contain "1", "2", "3", "4", or "5":[^1-5] • - The hyphen separates the beginning and ending of a range of characters. A match occurs if any of the characters within the range is present. See the example above.
|	A vertical bar separates two alternative values or sets of values. The output can match one or the other value. For example, the following regular expression matches output that contains either "abc" or "defg": abc|defg
( )	Parentheses allow you to create complex expressions. For example, the following complex expression matches on "abc", "abcabc", or "defg", but not on "abcdefgdefg": ((abc)+)|((defg)?)

If you want to filter for a special character instead of using the special character as described in the table above, enter a backslash (\ ) before the character. For example, to filter on output containing an asterisk, enter the asterisk portion of the regular expression as "*".

```
device#show ip route bgp | include \*
```

Displaying lines containing a specified string

The following command filters the output of the **show interface** command for port 3/11 to display only lines containing the word "Internet". This command can be used to display the IP address of the interface.

```
device#show interface e 3/11 | include Internet
  Internet address is 10.168.1.11/24, MTU 1518 bytes, encapsulation ethernet
```

Syntax: *show-command* | **include** *regular-expression*

NOTE
The vertical bar (**|**) is part of the command.

Note that the regular expression specified as the search string is case sensitive. In the example above, a search string of "Internet" would match the line containing the IP address, but a search string of "internet" would not.

Displaying lines that do not contain a specified string

The following command filters the output of the **show who** command to display only the lines that do not contain the word "closed". This command can be used to display open connections to the Brocade device.

```
device#show who | exclude closed
Console connections:
        established
        you are connecting to this session
        2 seconds in idle
Telnet connections (inbound):
 1      established, client ip address 10.168.9.37
        27 seconds in idle
Telnet connection (outbound):
SSH connections:
```

Syntax: *show-command* | **exclude** *regular-expression*

Displaying lines starting with a specified string

The following command filters the output of the **show who** command to display output starting with the first line that contains the word "SSH". This command can be used to display information about SSH connections to the Brocade device.

```
device#show who | begin SSH
SSH connections:
 1      established, client ip address 10.168.9.210
        7 seconds in idle
 2      closed
 3      closed
 4      closed
 5      closed
```

Syntax: *show-command* | **begin** *regular-expression*

Creating an alias for a CLI command

An alias serves as a shorthand version of a longer CLI command. For example, you can create an alias called *shoro* for the **show ip route** command. You can then enter te *shoro* alias at the command prompt and the **show ip route** command is issued.

To create an alias called *shoro* for the CLI command **show ip route**, enter the **alias shoro = show ip route** command.

```
device(config)# alias shoro = show ip route
```

Syntax: [no] alias *alias-name* **=** *cli-command*

The *alias-name* must be a single word, without spaces.

After the alias is configured, entering *shoro* in the privileged EXEC mode or in the global configuration mode issues the **show ip route** command.

Enter the command **copy running-config** with the appropriate parameters to create an alias called *wrsbc*.

```
device(config)#alias wrsbc = copy running-config tftp 10.10.10.10 test.cfg
```

To remove the *wrsbc* alias from the configuration, enter one of the following commands.

```
device(config)#no alias wrsbc
```

or

```
device(config)#unalias wrsbc
```

Syntax: unalias *alias-name*

The specified *alias-name* must be the name of an alias already configured on the Brocade device.

To display the aliases currently configured on the Brocade device, enter the following command in the Privileged EXEC mode or in the global configuration mode.

```
device# alias
          wrsbc      copy running-config tftp 10.10.10.10 test.cfg
          shoro       show ip route
```

Syntax: alias

Configuration notes for creating a command alias

The following configuration notes apply to this feature:

- You cannot include additional parameters with the alias at the command prompt. For example, after you create the *shoro* alias, *shoro bgp* would not be a valid command.
- If configured on the Brocade device, authentication, authorization, and accounting is performed on the actual command, not on the alias for the command.
- To save an alias definition to the startup-config file, use the **write memory** command.

Specifying stack-unit, slot number, and port number

Many CLI commands require users to enter port numbers as part of the command syntax, and many **show** command outputs display port numbers. Port numbers are entered and displayed in one of the following formats:

- port number only
- slot number and port number
- stack-unit, slot number, and port number

Not all formats are supported on all devices. To identify a port, refer to the labels on the front panel of the device.

Specifying a port on a modular device

On modular devices such as the FSX 800 and FSX 1600, you must specify the port number in the following format when you issue a command that requires a port parameter: *slot/port*.

The following example enters the ethernet interface sub-configuraton mode for the first port on a modular device.

```
device(config)#interface e 1/1
device(config-if-1/1)#
```

Specifying a port on stackable devices

On stackable devices (FCX and ICX) you must specify the port in the following format when you issue a command that requires a port parameter: *stack-unit /slot/port*.

The following example enters the ethernet interface sub-configuraton mode for the first port on a stackable device.

```
device(config)#interface e 1/1/1
device(config-if-e1000-1/1/1)#
```

Refer to "Brocade Stackable Devices" in the *FastIron Ethernet Switch Stacking Configuration Guide* for more information on stackable devices.

Commands F - J

failover

Enables or disables LAG (Link Aggregation Group) hardware failover on the next port in LAG or on all ports in LAG.

Syntax **failover** {**next** | **all**}

no failover {**next** | **all**}

Command Default LAG hardware failover is disabled.

Parameters

next

Specifies that failover is to be enabled or disabled on the next port in LAG.

all

Specifies that failover is to be enabled or disabled on all ports in LAG.

Modes Dynamic LAG configuration mode

Usage Guidelines The **no** form of this command disables LAG hardware failover.

LAG hardware failover is supported only on Brocade ICX 7750 devices.

Examples The following example enables LAG failover on the next port in LAG:

```
device(config)# lag one dynamic
device(config-lag-one)# failover next
```

The following example enables LAG failover on all ports in LAG:

```
device(config)# lag one dynamic
device(config-lag-one)# failover all
```

History

Release version	Command history
08.0.10	This command was introduced.

filter-strict-security enable

Enables or disables strict filter security for MAC authentication and dot1x authentication.

Syntax **filter-strict-security**

no filter-strict-security

Command Default MAC addresses are blocked.

Strict filter security is enabled for all 802.1X-enabled interfaces.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables strict filter security.

When strict filter security is enabled, authentication fails if the filters contain invalid information.

Use the **filter-strict-security enable** command at the configuration authentication level and the **auth filter-strict-security enable** command at the interface level.

When strict filter security is disabled:

- If the Filter-ID attribute in the Access-Accept message contains a value that does not refer to an existing filter (a MAC address filter or IP ACL is configured on the device), then the port is authenticated but no filter is dynamically applied to it.
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the port is authenticated but the filter specified in the Vendor-Specific attribute is not applied to the port.
- By default, strict security mode is enabled for all 802.1X-enabled interfaces, but you can manually disable or enable it, either globally or for specific interfaces.

Examples The following example enables strict filter security.

```
device(config)# authentication
device(config-authen)# filter-strict-security enable
```

History

Release version	Command history
08.0.20	This command was introduced.

flash

Use the **flash** command to perform basic flash file maintenance.

Syntax **flash** { **copy** *source-file destination-file* | **dbgflock** | **delete** *flash-file* | **files** *directory-name* | **rename** *source-file destination-file* }

Command Default N/A

Parameters

copy *source-file destination-file*

Copy the source flash file to a new file

dbgflock

Display the flash access lock holder

delete *flash-file*

Delete the flash file

files *directory-name*

Display flash files in a particular directory

rename *source-file destination-file*

Rename a flash file

Modes Exec mode

Usage Guidelines The command is useful in flash file maintenance.

Examples In the following example, flash files are displayed.

```
device# flash files
Type       Size   Name
----------------------
F        24108665 primary
F        24108665 secondary
F             610 startup-config.backup
F            2052 startup-config.txt

48219992 bytes 4 File(s) in FI root

     1768706048 bytes free in FI root
     1768706048 bytes free in /
```

The **show flash** command also displays flash file information but with different results.

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Sec Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
  Code Flash Free Space = 1768706048
```

History

Release version	Command history
8.0.10	This command was introduced.

flow-control

Enables or disables flow control and flow control negotiation, and advertises flow control.

Syntax **flow-control** [**neg-on**]

no flow-control [**neg-on**]

Command Default Flow control is enabled.

Parameters **neg-on**

Enables negotiation on an interface.

Modes Global configuration mode

Interface configuration mode

Usage Guidelines The **no** form of this command disables flow control.

On ICX 7750 devices the default packet-forwarding method is cut-through, in which port flow control (IEEE 802.3x) is not supported but priority-based flow control (PFC) is supported. You can configure the **store-and- forward** command in global configuration mode to enable the store-and-forward method for packet-forwarding.

By default, when flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

NOTE
Enabling only port auto-negotiation does not enable flow control negotiation. You must use the **flow-control neg-on** command to enable flow-control negotiation.

Examples The following example disables flow control globally.

```
Device(config)#no flow-control
```

The following example enables flow control on Ethernet ports 0/1/11 to 0/1/15.

```
Device(config)#interface ethernet 0/1/11 to 0/1/15
device(config-mif-0/1/11-0/1/15)#flow-control
```

The following example disables flow control on Ethernet port 1/1/9.

```
Device(config)# interface ethernet 1/1/9
Device(config-if-e1000-1/1/9)no flow-control
```

The following example enables flow-control negotiation on Ethernet interface 1/1/2.

```
Device(config)# interface ethernet 1/1/2
Device(config-if-e1000-1/1/2)flow-control neg-on
```

History

Release version	Command history
08.0.20	This command was modified. Enabling only auto-negotiation does not enable flow-control negotiation.

force-up ethernet

Forces the member port of a dynamic LAG (Link Aggregation Group) to be logically operational even if the dynamic LAG is not operating.

Syntax **force-up ethernet** *port*

no force-up ethernet *port*

Command Default The member ports of a dynamic LAG are logically operational only if the dynamic LAG is operating.

Parameters *port*

Specifies the port.

Modes Dynamic LAG configuration mode

Usage Guidelines The **no** form of the command causes the specified port to be logically operational only when the dynamic LAG is operating.

When the dynamic LAG is not operational, the port goes to "force-up" mode. In this mode, the port is logically operational, which enables a PXE-capable host to boot from the network using this port. Once the host successfully boots from the network, the dynamic LAG can connect the host to the network with the LAG link. Even if the dynamic LAG fails later, this port is brought back to "force-up" mode and remains logically operational.

A port that is in "force-up" mode has the operational status ("Ope") of "Frc". Use the **show lag** command to display the operational status.

If any port in a dynamic LAG receives an LACPDU, the port in force-up mode leaves force-mode and becomes a member port in the dynamic LAG.

Examples The following example enables PXE boot support on member port 3/1/1 of a dynamic LAG R4-dyn.

```
device(config)# lag R4-dyn
device(config-lag-R4-dyn)# force-up ethernet 3/1/1
```

History

Release version	Command history
08.0.01	This command was introduced.

graft-retransmit-timer

Configures the time between the transmission of graft messages sent by a device to cancel a prune state.

Syntax **graft-retransmit-timer** *seconds*

no graft-retransmit-timer *seconds*

Command Default The graft retransmission time is 180 seconds.

Parameters *seconds*

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default graft retransmission time, 180 seconds.

Messages sent by a device to cancel a prune state are called graft messages. When it receives a graft message, the device responds with a Graft Ack (acknowledge) message. If this Graft Ack message is lost, the device that sent it resends it.

Examples This example configures a graft retransmission timer to 90 seconds.

```
device(config)# router pim
device(config-pim-router)# graft-retransmit-timer 90
```

hardware-drop-disable

Disables passive multicast route insertion (PMRI).

Syntax **hardware-drop-disable**

no hardware-drop-disable

Command Default PMRI is enabled.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default and enables PMRI.

To prevent unwanted multicast traffic from being sent to the CPU, PIM routing and PMRI can be used together to ensure that multicast streams are forwarded out only on ports with interested receivers and unwanted traffic is dropped in hardware on Layer 3 switches. To disable this process, use the **hardware-drop-disable** command.

NOTE
Disabling hardware-drop does not immediately take away existing hardware-drop entries, they will go through the normal route aging processing when the traffic stops.

Examples This example disables PMRI.

```
device(config)#router pim
device(config-pim-router)# hardware-drop-disable
```

hello-interval

Sets the hello-interval in seconds or milliseconds for IPv4 VRRP and IPv6 VRRP.

Syntax **hello-interval** { *seconds* | *milliseconds* }

hello-interval msec *milliseconds*

no hello-interval

Command Default The hello-interval is 1 second.

Parameters *seconds*

Specifies the hello-interval in seconds from 1 through 40 seconds for IPv4 VRRP, IPv4 VRRPv3, VRRP-E, and IPv6 VRRP-E. The default is 1 second.

milliseconds

Specifies the hello-interval in seconds from 1 through 84 seconds for IPv4 VRRP, VRRP-E, and IPv6 VRRP-E and 1 through 40 seconds for IPv4 VRRPv3. The default is 1 second.

Modes VRRP virtual router ID configuration

Usage Guidelines IPv4 VRRPv2 supports the hello-interval configuration in seconds, while IPv6 VRRP supports this configuration in milliseconds; both use the CLI **hello-interval** . However, IPv4 VRRPv3 supports both the seconds and milliseconds configuration using the **hello-interval** command and the **hello-interval** command with the **msec** option.

Examples The following example configures the hello-interval on IPv4 VRRPv2 to 20 seconds.

```
device Router1(config)# interface ethernet 1/6
device Router1(config-if-1/6)# ipv4 vrrp vrid 1
device Router1(config-if-1/6-vrid-1)# hello-interval 20
```

The following example configures the hello-interval on IPv4 VRRPv3 to 200 milliseconds.

```
device Router1(config)# interface ethernet 1/6
device Router1(config-if-1/6)# ipv4 vrrp vrid 1
device Router1(config-if-1/6-vrid-1)# hello-interval msec 200
```

History

Release version	Command history
08.0.10	This command was introduced.

hello-timer

Configures the interval at which hello messages are sent out of Protocol Independent Multicast (PIM) interfaces.

Syntax **hello-timer** *seconds*

no hello-timer *seconds*

Command Default The hello interval is 30 seconds.

Parameters *seconds*

Specifies the interval in seconds. The range is 10 through 3600 seconds. The default is 30 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default hello interval, 30 seconds.

Devices use hello messages to inform neighboring devices of their presence.

Examples This example configures a hello interval of 120 seconds on all ports on a device operating with PIM.

```
device(config)# router pim
device(config-pim-router)# hello-timer 120
```

hitless-failover enable

Enables hitless stacking failover and switchover. The standby controller is allowed to take over the active role without reloading the stack when failover occurs.

Syntax **hitless-failover enable**

no hitless-failover enable

Command Default Hitless stacking failover is enabled. In earlier releases, failover and switchover were disabled by default.

Modes Global configuration mode

Usage Guidelines Use the **no** form of the command to disable hitless stacking failover. The change takes effect immediately.

The **hitless-failover enable** and **no hitless-failover enable** commands must be executed from the active stack controller.

You must assign a stack mac address to the device using the **stack mac address** command before you can execute the **hitless-failover enable** command.

Examples The following example enables hitless stacking switchover and failover on the active controller for the stack.

```
device(config)# hitless-failover enable
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Hitless failover is enabled by default.

inactivity-timer

Configures the time a forwarding entry can remain unused before the device deletes it.

Syntax **inactivity-timer** *seconds*

no inactivity-timer *seconds*

Command Default The default inactive time is 180 seconds.

Parameters *seconds*

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default inactive time, 180 seconds.

A device deletes a forwarding entry if the entry is not used to send multicast packets. The Protocol Independent Multicast (PIM) inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

Examples This example configures an inactive time to 90 seconds.

```
device(config)# router pim
device(config-pim-router)# inactivity-timer 90
```

inline power

Configures inline power on Power over Ethernet (PoE) ports in interface configuration mode and link aggregation group (LAG) secondary ports in global configuration mode.

Syntax **inline power ethernet** *interface* [**decouple-datalink**] [**power-by-class** *power-class*] [**power-limit** *power-limit*] [**priority** *priority -value*]

no inline power ethernet *interface* [**decouple-datalink**] [**power-by-class** *power-class*] [**power-limit** *power-limit*] [**priority** *priority -value*]

NOTE
The **ethernet***interface* pair of parameters is required only if you want to configure inline power on secondary ports (you must use global configuration mode to do this).

Parameters

ethernet
Specifies an ethernet interface. You can configure the **ethernet** keyword only in global configuration mode.

interface
Specifies the number of the ethernet interface. This is used only with the **ethernet** keyword.

decouple-datalink
Specifies decoupling of datalink and PoE so that datalink state changes do not affect the PoE state. You can configure the **decouple-datalink** keyword in global and interface configuration modes.

power-by-class
Specifies the power limit based on class value. The range is 0-4. The default is 0.

power-limit
Specifies the power limit based on actual power value in mW. The range is 1000-15400|30000mW. The default is 15400|30000mW. For PoH ports, the range is 1000-95000mW, and the default is 95000mW. The power-limit value is rounded to the nearest multiple of 5 on PoH ports.

priority
Specifies the priority for power management. The range is 1 (highest) to 3 (lowest). The default is 3.

Modes Global configuration mode

Interface configuration mode

Usage Guidelines You cannot configure inline power on PoE LAG ports in interface configuration mode because the interface-level configuration is not available in the CLI for LAG secondary ports. The **inline power ethernet** command enables you to configure inline power on secondary ports in global configuration mode.

The **decouple-datalink** keyword was introduced in Release 08.0.01 to support the inline-power functionality. The decouple-datalink functionality is not supported in releases earlier than Release 08.0.01.

WARNING
If you want to keep decoupling in place on a PoE port when you configure the **inline power ethernet** command to change its other parameters, (for example, priority) you must also configure the **decouple-datalink** keyword.

WARNING
If you downgrade to a release earlier than 08.0.01, you cannot use **inline power** commands that have the **decouple-datalink** keyword. Any **inline power** commands in the startup config will not be effective.

Examples

Configuring inline power on LAG ports

The following example configures inline power on LAG ports.

```
Device(config)# lag "mylag" static id 5
Device(config-lag-mylag)# ports ethernet 1/1/1 to 1/1/4
Device(config-lag-mylag)# primary-port 1/1/1
Device(config-lag-mylag)# deploy
LAG mylag deployed successfully!
Device(config)#inline power ethernet 1/1/1 power-by-class 3
Device(config)#inline power ethernet 1/1/2
Device(config)#inline power ethernet 1/1/3 priority 2
Device(config)#inline power ethernet 1/1/4 power-limit 12000
```

Decoupling of inline power and datalink operations on PoE LAG ports

The following example decouples the behavior of the PoE and the datalink operations for PoE LAG ports. After the optional **decouple-datalink** keyword in the **inline power ethernet** command is entered, the datalink operational behavior on a PoE port does not affect the power state of the powered device (PD) that is connecting to the port.

```
Device(config)#inline power ethernet 1/1/1 decouple-datalink power-by-class 3
Device(config)#inline power ethernet 1/1/2 decouple-
datalink
Device(config)#inline power ethernet 1/1/3 decouple-datalink priority 2
Device(config)#inline power ethernet 1/1/4 decouple-datalink power-limit 12000
Device(config)# lag "mylag" static id 5
Device(config-lag-mylag)# ports ethernet 1/1/1 to 1/1/4
Device(config-lag-mylag)# primary-port 1/1/1
Device(config-lag-mylag)# deploy
LAG mylag deployed successfully!
```

Decoupling of inline power and datalink operations on regular PoE ports

The following example decouples the behavior of the PoE and the datalink operations for regular PoE ports. After the optional **decouple-datalink** keyword in the **inline power** command is entered, the datalink operational behavior on a PoE port does not affect the power state of the powered device (PD) that is connecting to the port.

```
Device(config)# interface ethernet 1/1/1
Device(config-if-e1000-1/1/1)# inline power decouple-datalink power-by-class 3
Device(config-if-e1000-1/1/1)# interface ethernet 1/1/2
Device(config-if-e1000-1/1/2)# inline power decouple-datalink
Device(config-if-e1000-1/1/2)# interface ethernet
1/1/3
Device(config-if-e1000-1/1/3)# inline power decouple-datalink priority 2
Device(config-if-e1000-1/1/3)# interface ethernet 1/1/4
Device(config-if-e1000-1/1/4)# inline power decouple-datalink power-limit 12000
```

History

Release	Command History
08.0.01	This command was modified to run in global configuration mode using the **ethernet** keyword. The **decouple-datalink** keyword was also introduced.
08.0.20	This command was modified to allow requisite PoH power limits.

inline power install-firmware scp

Upgrades the PoE firmware of a Brocade SX module or FastIron stacking device by downloading a firmware file from an SCP server.

Syntax **inline power install-firmware** { **stack-unit** *unit-id* | **module** *module-id* } **scp** { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

stack-unit *unit-id*

Specifies the unit ID of the FastIron device in the stack to copy the PoE firmware. You must specify the stack unit when you configure the **inline power install-firmware** command to upgrade PoE firmware on a stacking device.

module *module-id*

Specifies the module ID of the Brocade SX device to copy the PoE firmware. You must specify the module when you configure the **inline power install-firmware** command to upgrade PoE firmware on a Brocade SX device.

ipv4-address-

Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-

Specifies the IP hostname of the SCP server.

ipv6

Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length

Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-

Specifies the IPv6 hostname of the SCP server.

outgoing-interface

Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*

Configures an Ethernet interface as the outgoing interface.

ve *ve-number*

Configures a virtual interface (VE) as the outgoing interface.

public-key

Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa

Specifies DSA as the public key authentication.

rsa

Specifies RSA as the public key authentication.

remote-port

Specifies the remote port number for the TCP connection.

remote-filename

Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

If you do not configure the type of public key authentication, the default authentication type is password.

You must specify the stack unit and module when you configure the **inline power install-firmware** command to upgrade PoE firmware on a stacking device.

Examples

This example upgrades the PoE firmware of a FastIron device by downloading a firmware file from an SCP server:

```
Device#inline power install-firmware stack-unit 2 scp 2.2.2.2
icx64xx_poeplus_02.1.0.b004.fw
```

History

Release version	Command history
08.0.20	This command was introduced.

ip arp inspection validate

Enables validation of the ARP packet destination MAC, ARP Packet IP, and source MAC addresses.

Syntax **ip arp inspection validate** [**dst-mac** | **ip** | **src-mac**]

Command Default IP ARP packet destination address validation is disabled.

Parameters

dst-mac

Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip

Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

src-mac

Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Modes Global configuration mode

Usage Guidelines You can enable validation of ARP packet destination addresses for a single destination address or for all destination addresses.

You must execute the command once for each type of ARP packet destination address you want to validate.

Examples The following example enables validation of the MAC, ARP Packet IP, and source MAC ARP packet destination addresses.

```
device(config)# configure terminal
device(config)# ip arp inspection validate dst-mac
device(config)# ip arp inspection validate src-mac
device(config)# ip arp inspection validate ip
```

History

Release version	Command history
08.0.10a	This command was introduced.

ip bootp-use-intf-ip

Configures a Dynamic Host Configuration Protocol (DHCP) relay agent to set the source IP address of a DHCP-client packet with the IP address of the interface in which the DHCP-client packet is received.

Syntax **ip bootp-use-intf-ip**

no ip bootp-use-intf-ip

Command Default The DHCP relay agent sets the source IP address of a DHCP-client packet with the IP address of the outgoing interface to the DHCP server.

Modes Global configuration mode

Usage Guidelines You can configure ACLs on a DHCP server to permit or block access to the DHCP server from particular subnets or networks. You can then use this command on the DHCP relay agent to reveal the source subnet or network of a DHCP packet to the DHCP server, which enables the DHCP server to process or discard the DHCP traffic according to the configured ACLs.

Examples The following example configures a FastIron DHCP relay agent so that it sets the source IP address of a DHCP-client packet with the IP address of the interface on which the DHCP-client packet is received.

```
device(config)# ip bootp-use-intf-ip
```

ip dscp-remark

Enables remarking of the differentiated services code point (DSCP) field for all IPv4 packets.

Syntax **ip dscp-remark** *dscp-value*

no ip dscp-remark *dscp-value*

Command Default DSCP remarking is disabled.

Parameters *dscp-value*

Specifies the DSCP value ranges you are remarking.

Modes Global configuration mode

Interface configuration mode

Usage Guidelines The **no** form of this command disables DSCP remarking.

In interface configuration mode, the command enables DSCP remarking for the given port. The configuration can be done on a physical port, LAG, and VE port.

Examples The following example globally enables DSCP remarking on all IPv4 packets when the DSCP bit value is 40:

```
Device(config)# ip dscp-remark 40
```

The following example enables DSCP remarking on all IPv4 packets received on a specific port when the DSCP bit value is 50:

```
Device(config)# interface ethernet1/1/1
Device(config-if-e1000-1/1/1)# ip dscp-remark 50
```

ip igmp group-membership-time

Specifies how long an IGMP group remains active on an interface in the absence of a group report.

Syntax **ip igmp group-membership-time** *num*

no ip igmp group-membership-time *num*

Command Default By default, a group will remain active on an interface for 260 seconds in the absence of a group report.

Parameters *num*

Number in seconds, from 5 through 26000.

Modes Global configuration mode.

Usage Guidelines The **no** form of this command resets the group membership time interval to the default of 260 seconds.

Group membership time defines how long a group will remain active on an interface in the absence of a group report.

Examples This example specifies an IGMP (V1 and V2) membership time of 240 seconds.

```
Device(config)# ip igmp group-membership-time 240
```

ip igmp max-response-time

Defines how long a device waits for an IGMP response from an interface before determining that the group member on that interface is down and removing the interface from the group.

Syntax **ip igmp max-response-time** *num*

no ip igmp max-response-time *num*

Command Default The device waits 10 seconds.

Parameters *num*

Number, in seconds, from 1 through 25. The default is 10.

Modes Global configuration mode.

Usage Guidelines The **no** form of this command resets the maximum response time interval to the default of 10 seconds.

Examples To define

This example changes the IGMP (V1 and V2) maximum response time to 8 seconds.

```
Device(config)# ip igmp max-response-time 8
```

ip igmp port-version

Configures an IGMP version recognized by a physical port that is a member of a virtual routing interface.

Syntax **ip igmp port-version** *version-number* **ethernet** *port-number* [**to ethernet** *port-number*[**ethernet** *port-number...*]]

no ip igmp port-version *version-number* **ethernet** *port-number* [**to ethernet** *port-number*[**ethernet** *port-number...*]]

Command Default IGMP Version 2 is enabled.

Parameters *version-number*

Specifies the version number: 1, 2, or 3. Version 2 is the default.

ethernet *port-number*

Specifies the physical port within a virtual routing interface.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command restores the default; IGMP Version 2 is enabled.

Examples This example enables IGMP Version 3 on a physical port that is a member of a virtual routing interface. It first enables IGMP Version 2 globally, then enables Version 3 on ports 1/3 through 1/7 and port e2/9. All other ports in this virtual routing interface are configured with IGMP Version 2.

```
device(config)#interface ve 3
device(config-vif-3)# ip igmp version 2
device(config-vif-3)# ip igmp port-version 3 e1/3 to e1/7 e2/9
```

ip igmp proxy

Configures IGMP proxy on an interface

Syntax **ip igmp proxy** [**group-filter***access-list*]

no ip igmp proxy [**group-filter***access-list*]

Command Default IGMP proxy is not enabled.

Parameters **group-filter**

Specifies filtering out groups in proxy report messages.

access-list

Specifies the access list name or number you want filtered out.

Modes Interface configuration mode.

Usage Guidelines The **no** form of this command disables IGMP proxy on an interface.

IGMP proxy is supported only in PIM dense environments where there are IGMP clients connected to the Brocade device. PIM DM must be enabled in passive mode.

IGMP proxy is not supported on interfaces on which PIM sparse mode (SM) or Source Specific Multicast (SSM) is enabled.

Enter the **ip igmp proxy** command without the **group-filter** keyword to remove the group-filter association without disabling the proxy.

Examples This example enables IGMP proxy on an interface. It first shows how to configure PIM globally, configure an IP address that will serve as the IGMP proxy for an upstream device on interface 1/3, enable PIM passive on the interface, and then enable IGMP proxy.

```
device(config)#router pim
device(config)#interface ethernet 1/3/3
device(config-if-e1000-1/3)#ip address 10.95.5.1/24
device(config-if-e1000-1/3)#ip pim passive
device(config-if-e1000-1/3)#ip igmp proxy
```

The following example filters out the ACL1 group in proxy report messages.

```
device(config)#router pim
device(config)#interface ethernet 1/3/3
device(config-if-e1000-1/3)#ip address 10.95.5.1/24
device(config-if-e1000-1/3)#ip pim passive
device(config-if-e1000-1/3)#ip igmp proxy group-filter ACL1
```

ip igmp query-interval

Defines how often a device queries an interface for IGMP group membership.

Syntax **ip igmp query-interval** *num*

no ip igmp query-interval *num*

Command Default The query interval is 125 seconds

Parameters *num*

Number in seconds, from 2 through 3600. The default is 125.

Modes Global configuration mode.

Usage Guidelines The **no** form of this command resets the query interval to the default of 125 seconds.

You must specify a query-interval value that is a little more than twice the group membership time. You can configure the `ip igmp group-membership-time` command to specify the IGMP group membership time.

Examples This example sets the IGMP query interval to 120 seconds.

```
Device(config)# ip igmp query-interval 120
```

ip igmp tracking

Enables tracking and fast leave on an interface.

Syntax **ip igmp tracking**

no ip igmp tracking

Command Default Tracking and fast leave are disabled.

Modes Interface configuration mode.

Usage Guidelines The **no** form of this command restores the default; tracking and fast leave are disabled.

The IGMP Version 3 fast leave feature is supported in include mode but does not work in exclude mode.

Examples This example enables tracking and fast leave on a virtual routing interface.

```
Device(config)# interface ve 13
Device(config-vif-13)# ip igmp tracking
```

This example enables tracking and fast leave on a physical interface.

```
Device(config)# i(config)#interface ethernet 1/2/2
Device(config-if-e10000-1/2/2)# ip igmp tracking
```

ip igmp version

Specifies the IGMP version on a device.

Syntax **ip igmp version** *version-number*

no ip igmp version *version-number*

Command Default IGMP Version 2 is enabled.

Parameters *version-number*

Specifies the version number: 1, 2, or 3. Version 2 is the default.

Modes Global configuration mode.

Interface configuration mode

Usage Guidelines If this **no** form of this command restores the default; IGMP Version 2 is enabled.

Configure the **ip igmp port-version** command to configure an IGMP version recognized by a physical port that is a member of a virtual routing interface

Examples The following example enables IGMP Version 3 globally.

```
device#configure terminal
device(config)#ip igmp version 3
```

The following example, in interface configuration mode, enables IGMP Version 3 for a physical port.

```
device#configure terminal
device(config)#interface ethernet 1/5
device(config-if-1/5)#ip igmp version 3
```

The following example, in interface configuration mode, enables IGMP Version 3 for a virtual routing interface on a physical port.

```
device#configure terminal
device(config)#interface ve 3
device(config-vif-1)#ip igmp version 3
```

ip max-mroute

Configures the maximum number of IPv4 multicast routes that are supported.

Syntax **ip max-mroute** *num*

no ip max-mroute *num*

Command Default No maximum number of supported routes is configured.

Parameters *num*

Configures the maximum number of multicast routes supported.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command restores the default (no maximum number of supported routes is configured).

Examples The following example configures the maximum number of 20 supported IPv4 multicast routes on the VRF named my_vrf.

```
Device(config)# vrf my_vrf
Device(config)# address-family ipv4
Device(config-vrf)# ip max-mroute 20
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute

Configures a directly connected static IPv4 multicast route.

Syntax **ip mroute** [**vrf** *vrf-name*] *ip-address ip-address mask* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

no ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask* { **ethernet** *stackid* / *slot* / *portnum*| **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default No static IPv4 multicast route is configured.

Parameters

vrf *vrf-name*
Configures a static mroute for this virtual routing and forwarding (VRF) route.

ip-address ip-address mask
Configures the destination IPv4 address and prefix for which the route should be added.

ethernet *stackid* / *slot* /*portnum*
Configures an Ethernet interface as the route path.

ve *num*
Configures a virtual interface as the route path.

tunnel *num*
Configures a tunnel interface as the route path.

cost
Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*
Configures the route's administrative distance. The range is 1-255; the default is 1.

name *name*
Name for this static route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command deletes a previously configured directly connected static multicast route.

Connected routes on PIM enabled interfaces are automatically added to the mRTM table.

Examples The following example configures a directly connected mroute to network 10.1.1.0/24 on interface ve 10.

```
Device(config-vrf)# ip mroute 10.1.1.0 255.255.255.0 ve 10
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute (next hop)

Configures a static IPv4 multicast route (mroute) with a next hop..

Syntax **ip mroute** [**vrf** *vrf-name*] *ip-address ip-address mask next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

no ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default No next-hop static IPv4 multicast route is configured.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

ip-address ip-address mask

Configures the destination IPv4 address and prefix for which the route should be added.

next-hop address

Configures a next-hop address as the route path.

cost

Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*

Configures the route's administrative distance. The range is 1 through 255; the default is 1.

name *name*

Name for this static route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command deletes a previously configured next-hop static IPv4 multicast route.

Examples The following example configures a next-hop static multicast IPv4 route to network 10.1.1.0/24 with next hop 10.2.1.1.

```
Device(config-vrf)# ip mroute 10.1.1.0 255.255.255.0 10.2.1.1
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute next-hop-enable-default

Enables the option to use the default multicast route (mroute) to resolve a static IPv4 mroute next hop.

Syntax **ip mroute** [**vrf** *vrf-name*] **next-hop-enable-default**

no ip mroute [**vrf** *vrf-name*] **next-hop-enable-default**

Command Default Static mroutes are not resolved using the default mroute.

Parameters **vrf** *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command disables the default IPv4 mroute option for next hops.

Examples The following example enables the use of the default mroute to resolve a static IPv4 mroute next hop:

```
Device(config-vrf)# ip mroute next-hop-enable-default
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute next-hop-recursion

Configures the recursion level when using static mroutes to resolve a static mroute next hop.

Syntax **ip mroute** [**vrf** *vrf-name*] **next-hop-recursion** *num*

no ip mroute [**vrf** *vrf-name*] **next-hop-recursion**

Command Default The recursion level for resolving a static mroute next hop is 3.

Parameters **vrf** *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

num

Specifies the recursion level used to resolve a static mroute next hop. The range of possible values is from 1 to 10. This is not used in the **no** form.

Modes VRF configuration mode

Usage Guidelines The **no** form restores the default recursion level for resolving a static mroute next hop, which is 3. You do not specify a value for the recursion level.

Examples The following example configures the recursion level for resolving a static mroute next hop to 7:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ip mroute next-hop-recursion 7
```

The following example configures the recursion level for resolving a static mroute next hop to 2:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ip mroute next-hop-recursion 2
```

The following example restores the default recursion level of 3 for resolving a static mroute next hop:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# no ip mroute next-hop-recursion
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip multicast

Configures the IGMP mode on a specific VLAN or on all VLANs on a device as active or passive.

Syntax **ip multicast** [**vlan** | *vlan-id*] [**active** | **passive**]

no ip multicast

Command Default IGMP mode is passive.

Parameters **vlan** *vlan-id*

Specifies a VLAN.

active

Configures IGMP active mode, that is, the device actively sends out IGMP queries to identify multicast groups on the network and makes entries in the IGMP table based on the group membership reports it receives.

passive

Configures IGMP passive mode, that is, the device does not send queries but forwards reports to the router ports that receive queries. When passive mode is configured on a VLAN, queries are forwarded to the entire VLAN.

Modes Global configuration mode

VLAN configuration mode

Usage Guidelines The **no** form of this command returns the device to the previous IGMP mode.

When entered without the **vlan** keyword, this command configures active or passive IGMP mode on all VLANs.

Routers in the network generally handle mode. Configure active IGMP mode only on a device is in a standalone Layer 2 Switched network with no external IP multicast router attachments. If you want to configure active IGMP mode on a device in such a network, you should do so on only one device and leave the others configured as passive.

The IGMP mode configured on a VLAN overrides the mode configured globally.

Examples The following example globally configures IGMP mode as active.

```
device#configure terminal
device(config)#ip multicast active
```

This example configures IGMP mode as active on VLAN 20.

```
device#configure terminal
device(config)#config vlan 20
device(config-vlan-20)#ip multicast active
```

ip multicast age-interval

Configures the time that group entries can remain in an IGMP group table on a specific VLAN or on all VLANs.

Syntax **ip multicast age-interval** [**vlan** *vlan-id*] *interval*

no ip multicast age-interval [**vlan** *vlan-id*] *interval*

Command Default Group entries can remain in the IGMP group table for up to 260 seconds.

Parameters **vlan** *vlan-id*

Specifies a VLAN.

interval

Specifies time, in seconds, that group entries can remain in the IGMP group table. The range is 20 through 26000 seconds. The default is 260 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default age interval to 260 seconds.

When entered without the **vlan** keyword, this command configures the time that group entries can remain in an IGMP group table on all VLANs.

When a device receives a group membership report it makes an entry for that group in the IGMP group table. You can configure the **ip multicast age-interval** to specify how long the entry can remain in the table before the device receives another group membership report. When multiple devices are connected, they must all be configured for the same age interval, which must be at least twice the length of the query interval, so that missing one report does not stop traffic.

Non-querier age intervals must be the same as the age interval of the querier.

Examples This example configures the IGMP group-table age interval to 280 seconds.

```
device#configure terminal
device(config)#ip multicast age-interval 280
```

ip multicast disable-flooding

Disables the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Syntax **ip multicast disable-flooding**

no ip multicast disable-flooding

Command Default The device floods unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Modes Global configuration mode

Usage Guidelines

NOTE
This command is supported as follows:

- On ICX 6650 devices
- From Release 8.0.10d, on ICX 7750 devices
- From Release 8.0.30, on ICX 7450 and ICX 7250 devices

NOTE
In Release 8.0.20, the **ip multicast disable-flooding** command is supported only on standalone ICX 7750 devices. In Release 8.0.30 and later releases, the **ip multicast disable-flooding** command is supported on both standalone and stacking ICX 7750 devices.

The **no** form of this command enables the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

After the hardware forwarding database (FDB) entry is made, the multicast traffic is switched only to the VLAN hosts that are members of the multicast group. This can avoid congestion and loss of traffic on the ports that have not subscribed to this IPv4 multicast traffic.

Examples The following example disables flooding of unregistered IPv4 multicast frames.

```
Brocade(config)# ip multicast disable-flooding
```

History

Release version	Command history
08.0.01	This command was introduced.
08.0.30	This command was modified to support ICX 7450 and ICX 7250 devices.

ip multicast leave-wait-time

Configures the wait time before stopping traffic to a port when a leave message is received.

Syntax **ip multicast leave-wait-time** *num*

no ip multicast leave-wait-time *num*

Command Default The wait time is 2 seconds.

Parameters *num*

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 1 through 5 seconds. The default is 2 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default wait time.

The device sends group-specific queries once per second to ask if any client in the same port still needs this group. Because of internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).

Examples This example configures the maximum time a client can wait before responding to a query to 1 second.

```
Device(config)#ip multicast leave-wait-time 1
```

ip multicast max-response-time

Sets the maximum number of seconds a client can wait before responding to a query sent by the device.

Syntax **ip multicast max-response-time** *interval*

no ip multicast max-response-time *interval*

Command Default The wait time is 10 seconds.

Parameters *interval*

Specifies the maximum time, in seconds, a client can wait before responding to a query sent by the switch. The range is 1 through 10 seconds. The default is 10 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default maximum interval.

Examples This example configures the maximum time a client can wait before responding to a query to 5 seconds.

```
Device(config)#ip multicast max-response-time 5
```

ip multicast mcache-age

Configures the time for an mcache to age out when it does not receive traffic.

Syntax **ip multicast mcache-age** *num*

no ip multicast mcache-age

Command Default The mcache ages out in 60 seconds.

Parameters *num*

Specifies the time, in multiples of 60 seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 60 through 3600 seconds, in multiples of 60. The default is 60 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default mcache age-out time.

Multicast traffic is hardware switched. One minute before aging out an mcache, the device mirrors a packet of this mcache to CPU to reset the age. If no data traffic arrives within 60 seconds, this mcache is deleted. Configuring a lower age-out time removes resources consumed by idle streams quickly, but it mirrors packets to CPU often. Configure a higher value only when data streams are arriving consistently.

Examples This example configures the time for an mcache to age out to 180 seconds.

```
Device(config)#ip multicast mcache-age 180
```

ip multicast query-interval

Configures how often the device sends general queries when IP multicast traffic reduction is set to active mode.

Syntax **ip multicast query-interval** *interval*

no ip multicast query-interval *interval*

Command Default The query interval is 125 seconds.

Parameters *interval*

Specifies the time, in seconds, between queries. The range is 10 through 3600 seconds. The default is 125 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the query interval to 125 seconds.

You can configure this command only when IP multicast traffic reduction is set to active IGMP snooping mode.

When multiple queries are connected, they must all be configured for the same interval.

Examples This example configures the time between queries to 120 seconds.

```
Device(config)#ip multicast query-interval 120
```

ip multicast report-control

Limits report forwarding within the same multicast group to no more than once every 10 seconds.

Syntax **ip multicast report-control**

no ip multicast report-control

Command Default A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default.

NOTE
This feature applies to IGMP V2 only. The leave messages are not rate limited.

This rate-limiting does not apply to the first report answering a group-specific query.

Configure this command to alleviate report storms from many clients answering the upstream router query.

The **ip multicast report-control** command was formerly named **ip igmp-report-control** . You can still configure the command as **ip igmp-report-control** ; however, it is renamed when you configure the **show configuration** command.

Examples This example limits the rate of report forwarding within the same multicast group.

```
Device(config)#ip multicast report-control
```

ip multicast verbose-off

Turns off the error or warning messages displayed by the device when it runs out of software resources or when it receives packets with the wrong checksum or groups.

Syntax **ip multicast verbose-off**

no ip multicast verbose-off

Command Default Error and warning messages are displayed.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores display of error and warning messages .

Error and warning messages are rate-limited.

Examples This example turns off error or warning messages .

```
Device(config)#ip multicast verbose-off
```

ip multicast version

Configures the IGMP version for snooping globally.

Syntax **ip multicast version** [**2** | **3**]

no ip multicast version

Command Default IGMP version 2 is configured.

Parameters **2**

Configures IGMP version 2.

3

Configures IGMP version 3.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the version to IGMP version 2.

If Layer 3 multicast routing is enabled on the device, Layer 2 IGMP snooping is automatically enabled.

See the description of the **multicast version** command for information on how to configure the IGMP version on a VLAN.

See the description of the **multicast port-version** command for information on how to configure the IGMP version on an individual port

Examples This example specifies IGMP version 3 on a device.

```
Device(config)#ip multicast version 3
```

ip multicast-nonstop-routing

Globally enables multicast non-stop routing for all virtual routing and forwarding (VRF) instances.

Syntax **ip multicast-nonstop-routing**

no ip multicast-nonstop-routing

Command Default Multicast non-stop routing is not enabled on VRFs.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default non-stop routing.

Examples The following example globally enables multicast non-stop routing for all VRFs.

```
device#configure terminal
device(config)#ip multicast-nonstop-routing
```

ip pcp-remark

Enables remarking of the priority code point (PCP) field in the VLAN header for all received tagged packets.

Syntax **ip pcp-remark** *pcp-value*

no ip pcp-remark *pcp-value*

Command Default PCP remarking is disabled.

Parameters *pcp-value*

Specifies the PCP value ranges you are remarking.

Modes Global configuration mode

Interface configuration mode

Usage Guidelines The **no** form of this command disables PCP remarking.

In Interface configuration mode, the command enables PCP remarking for each port. The command can be configured only on Layer 2 ports. The configuration can be done on a physical port, LAG, and VE port.

Examples The following example globally enables remarking of received tagged packets when the PCP bit value is 4.

```
Device(config)# ip pcp-remark 4
```

The following example enables remarking of received tagged packets on a specific port when the PCP bit value is 5.

```
Device(config)# interface ethernet1/1/1
Device(config-if-e1000-1/1/1)# ip pcp-remark 5
```

ip pim

Configures PIM in Dense mode on an interface.

Syntax **ip pim** [**passive**]

no ip pim [**passive**]

Command Default PIM is not enabled.

Parameters **passive**

Specifies PIM passive mode on the interface.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command disables PIM.

You must enable PIM globally before you enable it on an interface.

You must enable PIM on an interface before you can configure PIM passive on it.

Support for the **ip pim passive** command is implemented at Layer 3 interface (Ethernet or virtual Ethernet) level.

Because the loopback interfaces are never used to form PIM neighbors, the **ip pim passive** command is not supported on loopback interfaces.

The sent and received statistics of a PIM Hello message are not changed for an interface while it is configured as PIM passive.

Examples This example enables PIM globally, then enables it on interface 3.

```
Device(config)# router pim
Device(config-pim-router)# interface ethernet 1/1/3
Device(config-if-e10000-1/1/3)# ip address 207.95.5.1/24
Device(config-if-e10000-1/1/3)# ip pim
```

This example enables PIM passive on an interface.

```
Device(config)# router pim
device(config-pim-router)#exit
Device(config)#interface ethernet 2
Device(config-if-e1000-2)#ip pim
Device(config-if-e1000-2)#ip pim passive
Device(config-if-e1000-2)#exit
Device(config)#interface ve 2
Device(config-vif-2)#ip pim-sparse
Device(config-vif-2)#ip pim passive
Device(config-vif-2)#exit
```

ip pim border

Configures PIM parameters on an interface on a PIM Sparse border.

Syntax **ip pim border**

no ip pim border

Command Default The interface is not configured as a border device.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes the boundary on a PIM-enabled interface.

You can configure this command only in a PIM Sparse domain, that is, you must configure the **ip pim-sparse** command before you configure the **ip pim border** command.

Examples This example adds an IPv4 interface to port 1/2/2, enables PIM Sparse on the interface and configures it as a border device.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-1/2/2)# ip address 207.95.7.1 255.255.255.0
Device(config-if-e10000-1/2/2)# ip pim-sparse
Device(config-if-e10000-1/2/2)# ip pim border
```

ip pim dr-priority

Configures the designated router (DR) priority on IPv4 interfaces.

Syntax **ip pim dr-priority** *priority-value*

no ip pim dr-priority *priority-value*

Command Default The DR priority value is 1.

Parameters *priority-value*

Specifies the DR priority value as an integer. The range is 0 through 65535. The default is 1.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim dr-priority** command in either Dense mode (DM) or Sparse mode (SM).

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

Examples This example configures a DR priority value of 50.

```
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ip pim dr-priority 50
```

ip pim neighbor-filter

Determines which devices can become PIM neighbors.

Syntax **ip pim neighbor-filter** { *acl-name* | *acl-id* }

no ip pim neighbor-filter { *acl-name* | *acl-id* }

Command Default Neighbor filtering is not applied on the interface.

Parameters *acl-name*

Specifies an ACL as an ASCII string.

acl-id

Specifies either a standard ACL as a number in the range 1 to 99 or an extended ACL as a number in the range 100 to 199.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes any neighbor filtering applied on the interface.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim neighbor-filter** command in either Dense mode (DM) or Sparse mode (SM).

Configure the **access-list** command to create an access-control list (ACL)that specifies the devices you want to permit and deny participation in PIM

Examples This example prevents the host from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ip pim neighbor-filter
```

This example configures an ACL named 10 to deny a host and then prevents that host, 10.10.10.2, identified in that ACL from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# access-list  10  deny  host 10.10.10.2
Device(config)# access-list  10  permit any
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ip pim neighbor-filter 10
```

History

Release version	Command history
8.0.20a	This command was introduced.

ip pimsm-snooping

Enables PIM Sparse mode (SM) traffic snooping globally.

Syntax **ip pimsm-snooping**

no ip pimsm-snooping

Command Default PIM SM traffic snooping is disabled.

Modes Global configuration mode

VLAN configuration mode

Usage Guidelines The **no** form of this command disables PIM SM traffic snooping.

The device must be in passive mode before it can be configured for PIM SM snooping.

Use PIM SM snooping only in topologies where multiple PIM sparse routers connect through a device. PIM SM snooping does not work on a PIM dense mode router that does not send join messages and on which traffic to PIM dense ports is stopped. A PIM SM snooping-enabled device displays a warning if it receives PIM dense join or prune messages.

When PIM SM snooping is enabled globally, you can override the global setting and disable it for a specific VLAN.

Examples This example shows how to enable PIM SM traffic snooping.

```
Device(config)# ip pimsm-snooping
```

This example overrides the global setting and disable PIM SM traffic snooping on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)# no ip pimsm-snooping
```

ip pim-sparse

Enables PIM Sparse on an interface that is connected to the PIM Sparse network.

Syntax **ip pim-sparse** [**passive**]

no ip pim-sparse [**passive**]

Command Default PIM Sparse is not enabled on the interface.

Parameters **passive**

Specifies PIM passive mode on the interface.

Modes Interface configuration mode

Usage Guidelines The **no ip pim-sparse** command disables PIM Sparse.

The **no ip pim-sparse passive** command disables PIM passive mode on the interface.

You must enable PIM Sparse globally before you enable it on an interface.

If the interface is on the border of the PIM Sparse domain, you also must configure the **ip pim border** command.

Examples This example adds an IP interface to port 1/2/2, then enable PIM Sparse on the interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-2/2)# ip address 207.95.7.1 255.255.255.0
Device(config-if-e10000-2/2)# ip pim-sparse
```

ip ssh encryption disable-aes-cbc

Disables the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol.

Syntax **ip ssh encryption disable-aes-cbc**

no ip ssh encryption disable-aes-cbc

Command Default If JITC is enabled, only AES-CTR encryption mode is supported and AES-CBC mode is disabled by default. In the standard mode, the AES-CBC encryption mode is enabled.

Modes Global configuration mode

Usage Guidelines The **no** form of the command enables the AES-CBC encryption mode.

Examples The following example disables the AES-CBC encryption mode.

```
device(config)#  ip ssh encryption disable-aes-cbc
```

History

Release version	Command history
08.0.20a	This command was introduced.

ip ssl min-version

Configures the minimum TLS version to be used to establish the TLS connection.

Syntax **ip ssl min-version** { **tls_1_0** | **tls_1_1** | **tls_1_2** }

no ip ssl min-version { **tls_1_0** | **tls_1_1** | **tls_1_2** }

Command Default For devices which act as an SSL server or HTTPS server, the default connection is with TLS1.2.

For the Brocade device which acts as the SSL client or the syslog, OpenFlow, or secure AAA client, the TLS version is decided based on the server support.

Parameters

tls_1_0

Specifies TLS 1.0 as the minimum version.

tls_1_1

Specifies TLS 1.1 as the minimum version.

tls_1_2

Specifies TLS 1.2 as the minimum version.

Modes Global configuration mode

Usage Guidelines If **tls_1_1** is set as the minimum version, TLS 1.1 and later versions are supported.

The **no** form of the command removes the minimum TLS version configuration and supports all TLS versions.

Examples The following example establishes the TLS connection using the TLS 1.1 version and above.

```
device(config)# ip ssl min-version tls_1_1
```

History

Release version	Command history
08.0.20a	This command was introduced.

ipv6 max-mroute

Configures the maximum number of IPv6 multicast routes that are supported.

Syntax **ipv6 max-mroute** *num*

no ipv6 max-mroute *num*

Command Default No maximum number of supported routes is configured.

Parameters *num*

Configures the maximum number of multicast routes supported.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command restores the default (no maximum number of supported routes is configured).

Examples The following example configures the maximum number of 20 supported IPv6 multicast routes on the VRF named my_vrf.

```
Device(config)# vrf my_vrf
Device(config)# address-family ipv6
Device(config-vrf)# ipv6 max-mroute 20
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mld group-membership-time

Specifies the multicast listener discovery (MLD) group membership time for the default VRF or for a specified VRF.

Syntax **ipv6 mld group-membership-time** *num*

no ipv6 mld group-membership-time *num*

Command Default An MLD group will remain active on an interface in the absence of a group report for 260 seconds, by default.

Parameters *num*

Number in seconds, from 5 through 26000.

Modes Global configuration mode.

VRF configuration mode.

Usage Guidelines The **no** form of this command resets the group membership time interval to the default of 260 seconds.

Group membership time defines how long a group will remain active on an interface in the absence of a group report.

Examples This example specifies an MLD group membership time of 2000 seconds for the default VRF.

```
device# configure terminal
device(config)# ipv6 mld group-membership-time 2000
```

This example specifies an MLD group membership time of 2000 seconds for a specified VRF.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld group-membership-time 2000
```

ipv6 mld llqi

Configures the multicast listener discovery (MLD) last listener query interval.

Syntax **ipv6 mld llqi** *seconds*

no ipv6 mld llqi *seconds*

Command Default The MLD last listener query interval is 1 second.

Parameters *seconds*

specifies the number in seconds, of MLD group addresses available for all VRFs. The range is 1 through 25; the default is 1.

Modes Global configuration mode

VRF configuration mode

Usage Guidelines The **no** form of this command restores the default MLD last listener query interval.

Any MLD group memberships exceeding the group limit are not processed.

The last listener query interval is the maximum response delay inserted into multicast address-specific queries sent in response to Done messages, and is also the amount of time between multicast address-specific query messages. When a device receives an MLD Version 1 leave message or an MLD Version 2 state-change report, it sends out a query and expects a response within the time specified by the last listener query interval. Configuring a lower value for the last listener query interval allows members to leave groups faster.

Examples This example configures a last listener query interval of 5 seconds.

```
Device(config)# ipv6 mld llqi 5
```

This example configures a last listener query interval of 5 seconds for a VRF.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld llqi 5
```

ipv6 mld max-group-address

Configures the maximum number of MLD addresses for the default virtual routing and forwarding (VRF) instance or for a specified VRF.

Syntax **ipv6 mld max-group-address** *num*

no ipv6 mld max-group-address *num*

Command Default If this command is not configured, the maximum number of MLD addresses is determined by available system resources.

Parameters *num*

specifies the maximum number of MLD group addresses available for all VRFs. The range is 1 through 8192; the default is 4096.

Modes Global configuration mode

VRF configuration mode

Usage Guidelines If the **no** form of this command is configured, the maximum number of MLD addresses is determined by available system resources.

Any MLD group memberships exceeding the group limit are not processed.

Examples This example configures a maximum of 1000 IGMP addresses for the default VRF.

```
Device(config)# ipv6 mld max-group-address 1000
```

This example configures a maximum of 1000 IGMP addresses for the VRF named vpn1.

```
Device(config)# vrf vpn1
Device(config-vrf-vpn1)# address-family ipv4
Device(config-vrf-vpn1-ipv4)# ip igmp max-group-address 1000
```

ipv6 mld max-response-time

Configures the maximum time a multicast listener has to respond to queries for the default virtual routing and forwarding (VRF) instance or for a specified VRF.

Syntax **ipv6 mld max-response-time** *num*

no ipv6 mld max-response-time *num*

Command Default If this command is not configured, the maximum time a multicast listener has to respond to queries is 10 seconds.

Parameters *num*

specifies the maximum time, in seconds, a multicast listener has to respond. The range is 1 through 25; the default is 10.

Modes Global configuration mode

VRF configuration mode

Usage Guidelines If the **no** form of this command is configured, the maximum time a multicast listener has to respond to queries is 10 seconds.

Examples The following example configures the maximum time a multicast listener has to respond to queries to 20 seconds.

```
device# configure terminal
device(config)# ipv6 mld max-response-time 20
```

The following example configures the maximum time a multicast listener has to respond to queries to 20 seconds for the VRF named vpn1.

```
device# configure terminal
device(config)# vrf vpn1
Device(config-vrf-vpn1)# address-family ipv6
device(config)# ipv6 mld max-response-time 20
```

ipv6 mld port-version

Configures the multicast listening discovery (MLD) version on a virtual Ethernet interface.

Syntax **ipv6 mld port-version** *version-number*

no ipv6 mld port-version

Command Default The port uses the MLD version configured globally.

Parameters *version-number*

Specifies the MLD version, 1 or 2.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command restores the MLD version configured globally.

Examples This example configures MLD version 2 on virtual Ethernet interface 10.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld port-version 2
```

ipv6 mld query-interval

Configures the frequency at which multicast listening discovery (MLD) query messages are sent.

Syntax **ipv6 mld query-interval** *num*

no ipv6 mld query-interval *num*

Command Default 125 seconds

Parameters *num*

Number in seconds, from 2 through 3600. The default is 125.

Modes Global configuration mode.

VRF configuration mode.

Usage Guidelines The **no** form of this command resets the query interval to the default of 125 seconds.

You must specify a query-interval value that is greater than the interval configured by the `ipv6 mld max-response-time` command.

Examples This example sets the MLD query interval to 50 seconds.

```
Device(config)# ipv6 mld query-interval 50
```

This example sets the MLD query interval for a VRF to 50 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld query-interval 50
```

ipv6 mld robustness

Configures the number of times that the device sends each multicast listening discovery (MLD) message from an interface.

Syntax **ipv6 mld robustness** *num*

no ipv6 mld robustness *num*

Command Default The MLD robustness is 2 seconds.

Parameters *num*

Number in seconds, from 2 through 7. The default is 2.

Modes Global configuration mode.

VRF configuration mode.

Usage Guidelines The **no** form of this command resets the query interval to the default of 2 seconds.

Configure a higher value to ensure high MLD reliability.

Examples This example configures the MLD robustness to 3 seconds.

```
Device(config)# ipv6 mld robustness 3
```

This example configures the MLD robustness for a VRF to 3 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld robustness 3
```

ipv6 mld static-group

Configures one or more physical ports to be a permanent (static) member of a multicast listening discovery (MLD) group based on the range or count.

Syntax **ipv6 mld static-group** *multicast-group-addr* [**count** *count-number* | **to** *multicast-group-addr*] [**ethernet** *stackid\|slot\|portnum*] [**ethernet** *stackid\|slot\|portnum* **to ethernet** *stackid\|slot\|portnum*]]

no ipv6 mld static-group *multicast-group-addr* [**count** *count-number* | **to** *multicast-group-addr*] [**ethernet** *stackid\|slot\|portnum*] [**ethernet** *stackid\|slot\|portnum* **to ethernet** *stackid\|slot\|portnum*]]

Command Default The port is not added to MLD group.

Parameters *ip-addr*

The address of the static MLD group.

count *count-number*

Specifies the number of static MLD groups The range is 2 through 256.

to

Specifies a range of addresses.

ethernet *stackid\|slot\|portnum*

Specifies the ID of the physical port that will be a member of the MLD group. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can configure a single port or a list of ports, separated by a space.

Modes Interface configuration mode.

Usage Guidelines The **no** form of this command removes the port or ports from the MLD group.

You can specify as many port numbers as you want to include in the static group.

For a virtual routing interface (ve), specify the physical Ethernet ports on which to add the group address.

Examples The following example configures two static groups, starting from ff0d::1, without having to receive an MLDv1 report on a virtual Ethernet interface,

```
device# configure terminal
device(config)# interface ethernet 10000 1/1/2
device(config-if-e10000-1/1/2)# ipv6 mld static-group ff0d::1 count 2
```

The following example configures two static MLD groups, starting from ff0d::1, using the **to** keyword.

```
device# configure terminal
device(config)# interface ethernet 10000 1/1/2
device(config-if-e10000-1/1/2)# ipv6 mld static-group ff0d::1 to ff0d::2
```

The following example configures two static MLD groups on virtual ports starting from ff0d::1 using the **count** keyword.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 count 2 ethernet 1/5/2
```

The following example configures two static groups on virtual ports starting from ff0d::1 using the **to** keyword.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 to ff0d::2 ethernet 1/5/2
```

ipv6 mld tracking

Enables multicast listening discovery (MLD) tracking on a virtual interface.

Syntax **ipv6 mld tracking**

no ipv6 mld tracking

Command Default Multicast tracking is disabled on the virtual interface.

Modes Virtual interface configuration mode

Usage Guidelines The **no** form of this command restores the default; tracking is disabled.

When MLD tracking is enabled, a Layer 3 device tracks all clients that send membership reports. When a Leave message is received from the last client, the device immediately stops forwarding to the physical port, without waiting 3 seconds to confirm that no other clients still want the traffic.

Examples This example enables multicast tracking on a virtual interface.

```
device# configure terminal
device(config)# interface ve 13
device(config-vif-13)# ipv6 mld tracking
```

ipv6 mroute

Configures a static IPv6 route to direct multicast traffic along a specific path.

Syntax **ipv6 mroute** [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

no ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default No static IPv6 multicast route is configured.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

ipv6-address-prefix/prefix-length

Configures the destination IPv6 address and prefix for which the route should be added.

ethernet *stackid* / *slot* /*portnum*

Configures an Ethernet interface as the route path.

ve *num*

Configures a virtual interface as the route path.

tunnel *num*

Configures a tunnel interface as the route path.

cost

Configures a metric for comparing the route to other static routes in the IPv6 static route table that have the same destination. The range is 1 to 16; the default is 1.

distance *distance-value*

Configures the route's administrative distance. The range is 1 to 255; the default is 1.

name *name*

Name for this static route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command deletes a previously configured static multicast route.

Connected routes on PIM enabled interfaces are automatically added to the mRTM table.

Examples The following example configures a static IPv6 mroute to directly connected network 2020::0/120 on virtual interface ve 130.

```
Device(config-vrf)# ipv6 mroute 2020::0/120 ve 130
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute (next hop)

Configures a static IPv6 multicast route (mroute) with a next hop.

Syntax **ipv6 mroute** [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

no ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default No next-hop static IPv6 multicast route is configured.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

ipv6-address-prefix/prefix-length

Configures the destination IPv6 address and prefix for which the route should be added.

next-hop address

Configures a next-hop address as the route path.

cost

Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*

Configures the route's administrative distance. The range is 1 to 255; the default is 1.

name *name*

Name for this static route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command deletes a previously configured next-hop static IPv6 multicast route.

Examples The following example configures a next-hop static multicast IPv6 route to network 2020::0/120 with 2022::0/120 as the next hop.

```
Device(config-vrf)# ipv6 mroute 2020::0/120 2022::0/120
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute next-hop-enable-default

Enables the option to use the default multicast route (mroute) to resolve a static IPv6 mroute next hop.

Syntax **ipv6 mroute** [**vrf** *vrf-name*] **next-hop-enable-default**

no ipv6 mroute [**vrf** *vrf-name*] **next-hop-enable-default**

Command Default Static mroutes are not resolved using the default mroute.

Parameters **vrf** *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

Modes VRF configuration mode

Usage Guidelines The **no** form of this command disables the default IPv6 mroute option for next hops.

Examples The following example enables the use of the default mroute to resolve a static IPv6 mroute next hop:

```
Device(config-vrf)# ipv6 mroute next-hop-enable-default
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute next-hop-recursion

Configures the recursion level when using static mroutes to resolve a static mroute next hop.

Syntax **ipv6 mroute** [**vrf** *vrf-name*] **next-hop-recursion** *num*

no ipv6 mroute [**vrf** *vrf-name*] **next-hop-recursion**

Command Default The recursion level for resolving a static mroute next hop is 3.

Parameters **vrf** *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

num

Specifies the recursion level used to resolve a static mroute next hop. The range of possible values is from 1 to 10. This is not used in the **no** form.

Modes VRF configuration mode

Usage Guidelines The **no** form restores the default recursion level for resolving a static mroute next hop, which is 3. You do not specify a value for the recursion level.

Examples The following example configures the recursion level for resolving a static mroute next hop to 7:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ipv6 mroute next-hop-recursion 7
```

The following example configures the recursion level for resolving a static mroute next hop to 2:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ipv6 mroute next-hop-recursion 2
```

The following example restores the default recursion level of 3 for resolving a static mroute next hop:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# no ipv6 mroute next-hop-recursion
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 multicast age-interval

Configures the time that group entries can remain in a multicast listening discovery (MLD) group table.

Syntax **ipv6 multicast age-interval** *interval*

no ipv6 multicast age-interval *interval*

Command Default Group entries can remain in the MLD group table for up to 260 seconds.

Parameters *interval*

Specifies the time, in seconds, that group entries can remain in the MLD group table. The range is 20 through 7200 seconds. The default is 260 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default age interval to 260 seconds.

When a device receives a group membership report it makes an entry for that group in the MLD group table. You can configure the **ipv6 multicast age-interval** to specify how long the entry can remain in the table before the device receives another group membership report. When multiple devices are connected, they must all be configured for the same age interval, which must be at least twice the length of the query interval, so that missing one report does not stop traffic.

Non-querier age intervals must be the same as the age interval of the querier.

Examples This example configures the MLD group-table age interval to 280 seconds.

```
Device(config)#ipv6 multicast age-interval 280
```

ipv6 multicast disable-flooding

Disables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

Syntax **ipv6 multicast disable-flooding**

no ipv6 multicast disable-flooding

Command Default The device floods unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

Modes Global configuration mode

Usage Guidelines

NOTE
This command is supported only on ICX 6650 devices and, in Release 8.0.10d and later releases, on ICX 7750 devices.

NOTE
In Release 8.0.20, the **ipv6 multicast disable-flooding** command is supported only on standalone ICX 7750 devices. In Release 8.0.30 and later releases, the **ipv6 multicast disable-flooding** command is supported on both standalone and stacking ICX 7750 devices.

The **no** form of this command enables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

After the hardware forwarding database (FDB) entry is made, the multicast traffic is switched only to the VLAN hosts that are members of the multicast group. This can avoid congestion and loss of traffic on the ports that have not subscribed to this IPv6 multicast traffic.

Examples The following example disables flooding of unregistered IPv6 multicast frames.

```
Brocade(config)# ipv6 multicast disable-flooding
```

History

Release version	Command history
08.0.01	This command was introduced.
08.0.10d	This command was modified to support ICX 7750 devices.

ipv6 multicast leave-wait-time

Configures the wait time before stopping traffic to a port when a leave message is received.

Syntax **ipv6 multicast leave-wait-time** *num*

no ipv6 multicast leave-wait-time *num*

Command Default The wait time is 2 seconds.

Parameters *num*

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 1 through 5 seconds. The default is 2 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default wait time.

The device sends group-specific queries once per second to ask if any client in the same port still needs the group. Because of internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).

Examples This example configures the maximum time a client can wait before responding to a query as 1 second.

```
Device(config)#ipv6 multicast leave-wait-time 1
```

ipv6 multicast mcache-age

Configures the time for an mcache to age out when it does not receive traffic.

Syntax **ipv6 multicast mcache-age** *num*

no ipv6 multicast mcache-age *num*

Command Default The mcache ages out in 60 seconds.

Parameters *num*

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 60 through 3600 seconds. The default is 60 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default mcache age-out time.

You can set the time for a multicast cache (mcache) to age out when it does not receive traffic. Two seconds before an mcache is aged out, the device mirrors a packet of the mcache to the CPU to reset the age. If no data traffic arrives within two seconds, the mcache is deleted.

NOTE
On devices like FSX and ICX 7750, on which MAC-based MLD snooping is supported, more than one mcache can be mapped to the same destination MAC. Therefore, when an mcache entry is deleted the MAC entry may not be deleted. If you configure a lower value, the resource consumed by idle streams is quickly removed, but packets are mirrored to the CPU more frequently. Configure a higher value only when data streams are arriving consistently.

Examples This example configures the time for an mcache to age out to 180 seconds.

```
Device(config)#ipv6 multicast mcache-age 180
```

ipv6 multicast query-interval

Configures how often the device sends group membership queries when the multicast listening discovery (MLD) mode is set to active.

Syntax **ipv6 multicast query-interval** *interval*

no ipv6 multicast query-interval *interval*

Command Default Queries are sent every 125 seconds.

Parameters *interval*

Specifies the time, in seconds, between queries. The range is 10 through 3600 seconds. The default is 125 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the query interval to 125 seconds.

If the MLD mode is set to active, you can modify the query interval, which specifies how often the Brocade device sends group membership queries. When multiple queriers connect together, all queriers should be configured with the same interval.

Examples The following example configures the query interval to 120 seconds.

```
device#configure terminal
device(config)#ipv6 multicast query-interval 120
```

ipv6 multicast report-control

Limits report forwarding within the same group to no more than once every 10 seconds.

Syntax **ipv6 multicast report-control**

no ipv6 multicast report-control

Command Default A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default.

NOTE
This feature applies only to multicast listening discovery (MLD) version 1. The leave messages are not rate limited.

This rate-limiting does not apply to the first report answering a group-specific query.

Configure this command to alleviate report storms from many clients answering the upstream router query.

Examples This example limits the rate that reports are forwarded.

```
Device(config)#ipv6 multicast-report-control
```

ipv6 multicast verbose-off

Turns off error or warning messages that are displayed when the device runs out of software resources or when it receives packets with the wrong checksum or groups.

Syntax **ipv6 multicast verbose-off**

no ipv6 multicast verbose-off

Command Default Messages are displayed.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default display of messages.

Examples This example turns off the display of messages.

```
device# configure terminal
device(config)# ipv6 multicast verbose-off
```

ipv6 multicast version

Configures the multicast listening discovery (MLD) version for snooping globally.

Syntax **ipv6 multicast version** [**1** | **2**]

no ipv6 multicast version

Command Default MLD version 1 is configured.

Parameters

1

Configures MLD version 1.

2

Configures MLD version 2.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the version to MLD version 1.

You can configure the MLD version for individual VLANs, or individual ports within VLANs. If no MLD version is specified for a VLAN, the globally configured MLD version is used. If an MLD version is specified for individual ports in a VLAN, those ports use that version instead of the version specified for the VLAN or the globally specified version. The default is MLD version 1.

Examples This example specifies MLD version 2 on a device.

```
Device(config)#ipv6 multicast version 2
```

ipv6 multicast-boundary

Defines multicast boundaries for PIM-enabled interfaces.

Syntax **ipv6 multicast-boundary** *acl-spec*

no ipv6 multicast-boundary *acl-spec*

Command Default Boundaries are not defined.

Parameters *acl-spec*

Specifies the number or name identifying an access control list (ACL) that controls the range of group addresses affected by the boundary.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes the boundary on a PIM-enabled interface.

You can use standard ACL syntax to configure an access list.

Examples This example defines a boundary named MyAccessList for a PIM-enabled interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e1000-1/2)#ipv6 multicast-boundary MyAccessList
```

ipv6 nd router-preference

Configures the IPv6 router advertisement preference value to low or high (medium is the default). IPv6 router advertisement preference enables IPv6 router advertisement (RA) messages to communicate default router preferences from IPv6 routers to IPv6 hosts in network topologies where the host has multiple routers on its Default Router List.

Syntax **ipv6 nd router-preference** [**low** | **medium** | **high**]

no ipv6 nd router-preference [**low** | **medium** | **high**]

Command Default The IPv6 router advertisement preference value is set to medium.

Parameters

low

The two-bit signed integer (11) indicating the preference value "low".

medium

The two-bit signed integer (00) indicating the preference value "medium". This is the default preference value.

high

The two-bit signed integer (01) indicating the preference value "high".

Modes Interface configuration mode

Usage Guidelines The **no** form disables IPv6 router preference.

Examples The following example configures IPv6 RA preference for IPv6 routers:

```
device #configure terminal
device (config)# interface ethernet 2/3
device (config-if-eth2/3)# ipv6 nd router-preference low
```

History

Release version	Command history
08.0.10	This command was introduced.

ipv6 nd skip-interface-ra

Disables the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

Syntax **ipv6 nd skip-interface-ra**

no ipv6 nd skip-interface-ra

Command Default The IPv6-enabled interface sends the default IPv6 Router Advertisement (RA) messages. The IPv6 VRRP or VRRP-E instance configured on the interface also sends its virtual-IPv6 RA messages on the same interface. A connected IPv6 host receives these two different IPv6 RA messages with the same source address from this IPv6 router interface.

Modes Interface configuration mode

Usage Guidelines

NOTE
This command is valid only on an interface configured with IPv6 VRRP or VRRP-E.

The **no** form of this command enables the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

By default, all IPv6-enabled interfaces send IPv6 Router Advertisement (RA) messages. If you configure an IPv6 VRRP or VRRP-E instance on an interface, the VRRP/ VRRP-E instance also sends its IPv6 RA messages for the virtual IPv6 address on the same interface with the same source address. An IPv6 host cannot identify the valid IPv6 address for this router interface because of these two different IPv6 RA messages with the same source address from the same IPv6 router interface. To avoid this, run this command to disable the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

Examples The following example disables the default interface-level IPv6 RA messages on an ethernet interface 1/1/7 configured with IPv6 VRRP or VRRP-E.

```
device(config)# interface ethernet 1/1/7
device(config-if-e1000-1/1/7)# ipv6 address 2002:AB3::2/64
device(config-if-e1000-1/1/7)# ipv6 nd  skip-interface-ra
```

History

Release version	Command history
08.0.01	This command was introduced.

ipv6 neighbor inspection

Configures the static neighbor discovery (ND) inspection entries.

Syntax **ipv6 neighbor inspection** *ipv6-address mac-address*

no ipv6 neighbor inspection *ipv6-address mac-address*

Command Default Static ND inspection entries are not configured.

Parameters *ipv6-address*

Configures the IPv6 address of the host.

mac-address

Configures the MAC address of the host.

Modes Global configuration mode

VRF configuration mode

Usage Guidelines Use the **ipv6 neighbor inspection** command to manually configure static ND inspection entries for hosts on untrusted ports. During ND inspection, the IPv6 address and MAC address entries in the ND inspection table are used to validate the packets received on untrusted ports.

The **no** form of the command disables static ND inspection entries.

Examples The following example displays the configuration of a static ND inspection entry.

```
device(config)# ipv6 neighbor inspection 2001::1 0000.1234.5678
```

The following example displays the configuration of a static ND inspection entry for VRF 3.

```
device(config)# vrf 3
device(config-vrf-3)# ipv6 neighbor inspection 2001::100 0000.0000.4567
```

History

Release version	Command history
08.0.20	This command was introduced.

ipv6 neighbor inspection vlan

Configures and enables neighbor discovery (ND) inspection on a VLAN to inspect the IPv6 packets from untrusted ports.

Syntax **ipv6 neighbor inspection vlan** *vlan-number*

no ipv6 neighbor inspection vlan *vlan-number*

Command Default IPv6 neighbor inspection is not enabled.

Parameters *vlan-number*

Configures the ID of the VLAN.

Modes Global configuration mode

VRF configuration mode

Usage Guidelines When you configure this command, IPv6 packets from untrusted ports on the VLAN undergo ND inspection.

The **no** form of the command disables ND inspection.

Examples The following example enables ND inspection on VLAN 10.

```
device(config)# ipv6 neighbor inspection vlan 10
```

The following example enables ND inspection on VLAN 10 of VRF 3.

```
device(config)# vrf 3
device(config-vrf-3)# ipv6 neighbor inspection vlan 10
```

History

Release version	Command history
08.0.20	This command was introduced.

ipv6 pim border

Configures an interface to be on a PIM Sparse domain border.

Syntax **ipv6 pim border**

no ipv6 pim border

Command Default The interface is not configured as a border device.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes the boundary on a PIM-enabled interface.

You must enable PIM globally before you enable it on an interface.

Examples This example configures Ethernet interface 3/2/4 to be on a PIM Sparse domain border.

```
device(config) interface ethernet 3/2/4
Device(config-if-e10000-3/2/4)# ipv6 pim border
```

ipv6 pim dr-priority

Configures the designated router (DR) priority on IPv6 interfaces.

Syntax **ipv6 pim dr-priority** *priority-value*

no ipv6 pim *priority-value*

Command Default The DR priority value is 1.

Parameters *priority-value*

Specifies the DR priority value as an integer. The range is 0 through 65535. The default is 1.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IPv6 address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IPv6 address on the subnet is declared the DR regardless of the DR priority values.

Examples This example configures a DR priority value of 50 on Ethernet interface 3/2/4.

```
device(config) interface ethernet 3/2/4
Device(config-if-e10000-3/2/4)# ipv6 pim dr-priority 50
```

This example configures a DR priority value of 50 on a virtual Ethernet interface.

```
Device(config)# interface ve 10
Device(config-vif-10)# ipv6 pim dr-priority 50
```

ipv6 pim neighbor-filter

Determines which devices can become PIM neighbors.

Syntax **ipv6 pim neighbor-filter** *acl-name*

no ipv6 pim *acl-name*

Command Default Neighbor filtering is not applied on the interface.

Parameters *acl-name*

Specifies the access-control list (ACL)that identifies the devices you want to permit and deny participation in PIM.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes any neighbor filtering applied on the interface.

You must enable PIM globally before you enable it on an interface.

You can configure the **ipv6 pim neighbor-filter** command in either Dense mode (DM) or Sparse mode (SM).

Configure the **access-list** command to create an ACL defining the devices you want to permit and deny participation in PIM.

Examples This example prevents the host from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ipv6 pim neighbor-filter
```

This example configures an ACL named 10 to deny a host and then prevents that host, 1001::1/96, identified in that ACL from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# access-list 10  deny host 1001::1/96
Device(config)# access-list 10 permit any
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ipv6 pim neighbor-filter 10
```

History

Release version	Command history
8.0.20a	This command was introduced.

ipv6 pim-sparse

Enables PIM Sparse on an IPv6 interface.

Syntax **ipv6 pim-sparse**

no ipv6 pim-sparse

Command Default PIM Sparse is not enabled on the IPv6 interface.

Modes Interface configuration mode

Usage Guidelines The **no ipv6 pim-sparse** command removes the PIM sparse configuration from the IPv6 interface.

Examples This example adds an IPv6 interface to port 1/2/2, then enables PIM Sparse on the interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-2/2)# ipv6 address a000:1111::1/64
Device(config-if-e10000-2/2)# ipv6 pim-sparse
```

ipv6 raguard policy

Configures the specified Router Advertisement (RA) guard policy and enters RA guard policy configuration mode.

Syntax **ipv6 raguard policy** *name*

no ipv6 raguard policy *name*

Parameters *name*

An ASCII string indicating the name of the RA guard policy to configure.

Modes Global configuration mode

RA guard policy configuration mode

Usage Guidelines You can configure up to 256 RA guard policies.

The **no** form of this command deletes the specified RA guard policy.

Examples The following example configures an RA guard policy and enters RA guard policy configuration mode:

```
Brocade(config)# ipv6 raguard policy policy1
Brocade(ipv6-RAG-policy policy1)#
```

ipv6 raguard vlan

Associates a Router Advertisement (RA) guard policy with a VLAN.

Syntax **ipv6 raguard vlan** *vlan-number* **policy** *name*

no ipv6 raguard vlan *vlan-number* **policy** *name*

Parameters *vlan-number*

Configures the ID number of the VLAN to which the specified RA guard policy should be associated. Valid range is from 1 to 4095.

policy

Associates a RA guard policy to the VLAN.

name

Specifies the name of the RA guard policy to be associated with the VLAN.

Modes Global configuration mode

Usage Guidelines A VLAN can have only one association with a RA guard policy. If you try to associate a new RA guard policy with a VLAN that is already associated with a policy, the new RA guard policy replaces the old one.

Examples The following example associates RA guard policy named p1 with VLAN 1:

```
Brocade(config)# ipv6 raguard vlan 1 policy p1
```

ipv6 raguard whitelist

Configures the Router Advertisement (RA) guard whitelist and adds the IPv6 address as the allowed source IP address.

Syntax **ipv6 raguard whitelist** *whitelist-number* **permit** *ipv6-address*

no ipv6 raguard whitelist *whitelist-number* **permit** *ipv6-address*

Parameters *whitelist-number*

Configures the unique identifier for the RA guard whitelist. Valid values are 0 to 255.

permit

Configures the specified IPv6 address as the allowed source IP address to the RA guard whitelist.

ipv6-address

Configures the source IPv6 address. The address should be in the format X:X::X:X or X:X::X:X/M.

Modes Global configuration mode

Usage Guidelines You can configure source IP addresses from which RAs are permitted.

You can configure up to 64 RA guard whitelists, and each whitelist can have a maximum of 128 entries.

To remove the RA guard whitelist, use the **no** form the command without the **permit** keyword.

To remove a particular IPv6 address from the whitelist, use the **no** form of the command with the **permit***ipv6-address* keyword-variable pair.

When a whitelist associated with an RA guard policy is removed, all the entries in the whitelist are also removed. All the RAs are dropped because there is no whitelist associated with the RA guard policy.

Examples The following example configures an RA guard whitelist with the allowed source IP address:

```
Brocade(config)# ipv6 raguard whitelist 1 permit fe80:db8::db8:10
```

The following example removes an RA guard whitelist:

```
Brocade(config)# no ipv6 raguard whitelist 1
```

The following example removes a particular IPv6 address from the RA guard whitelist:

```
Brocade(config)# no ipv6 raguard whitelist 1 permit fe80:db8::db8:10
```

ipv6 router pim

Enables IPv6 PIM-Sparse mode for IPv6 routing globally or on a specified VRF.

Syntax **ipv6 router pim** [**vrf** *vrf-name*]

no ipv6 router pim [**vrf** *vrf-name*]

Command Default IPv6 PIM-Sparse mode is not enabled.

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

Modes Global configuration mode.

VRF configuration mode.

Usage Guidelines The **no** form of this command removes the IPv6 PIM-Sparse mode configuration.

Examples The following example enables IPv6 PIM-Sparse mode on a VRF named blue.

```
Device(config)# ipv6 router pim vrf blue
```

ipv6-address auto-gen-link-local

Generates a virtual link-local IPv6 address and assigns it as the virtual IPv6 address for a VRRPv3 instance.

Syntax **ipv6-address auto-gen-link-local**

no ipv6-address auto-gen-link-local

Modes VRRP sub-configuration mode

Usage Guidelines The **no** form of this command deletes the auto-generated virtual link-local IPv6 address for the VRRP v3 instance.

The default VRRPv3 implementation allows only the link-local address that is configured on a physical interface to be used as the virtual IPv6 address of a VRRPv3 instance. This limits configuring a link-local address for each VRRP instance on the same physical interface because there can be only one link-local address per physical interface. You can use this command on the owner or backup router to generate a virtual link-local IPv6 address from the virtual MAC address of a VRRPv3 instance and assign it as the virtual IPv6 address for the VRRPv3 instance. This auto-generated link-local IPv6 address is not linked to any physical interface on the router.

Examples The following example generates a virtual link-local IPv6 address and its allocation as the virtual IPv6 address of a VRRPv3 cluster on an owner router.

```
device(config)# interface ve 3
device(config-vif-3)# ipv6 vrrp vrid 2
device(config-vif-3-vrid-2)# owner
device(config-vif-3-vrid-2)# ipv6-address auto-gen-link-local
device(config-vif-3-vrid-2)# activate
```

History

Release version	Command history
08.0.01	This command was introduced.

ipv6-neighbor inspection trust

Enables trust mode for specific ports.

Syntax **ipv6-neighbor inspection trust** [**vrf** *vrf-name*]

no ipv6-neighbor inspection trust [**vrf** *vrf-name*]

Command Default Trust mode is not enabled. When you enable ND inspection on a VLAN, by default, all the interfaces and member ports are considered as untrusted.

Parameters **vrf**

Specifies the VRF instance.

vrf-name

Specifies the ID of the VRF instance.

Modes Interface configuration mode

VRF configuration mode

Usage Guidelines The **no** form of the command disables trust mode on ports.

Examples The following example displays the trust mode configuration for ports.

```
device(config)# interface ethernet 1/1/3
device(config-if-e1000-1/1/3)# ipv6-neighbor inspection trust
```

The following example displays the trust mode configuration on a port on VRF 3.

```
device(config-if-e1000-1/1/1)# ipv6-neighbor inspection trust vrf 3
```

History

Release version	Command history
08.0.20	This command was introduced.

jitc enable

Enables the Joint Interoperability Test Command (JITC) mode.

Syntax **jitc enable**

no jitc enable

Command Default JITC is not enabled.

Modes Global configuration mode

Usage Guidelines When JITC is enabled, the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol is disabled and the AES-CTR (Counter) encryption mode is enabled.

When JITC is enabled, the MD5 authentication scheme for NTP is disabled.

The **no** form of the command disables the JITC mode and puts the system back to the standard mode and enables both AES-CBC encryption mode and MD5 authentication configuration.

Examples The following example enables the JITC mode.

```
device(config)# jitc enable
```

History

Release version	Command history
08.0.20a	This command was introduced.

jitc show

Displays the status of the JITC mode.

Syntax **jitc show**

Modes Global configuration mode

Privileged EXEC mode

Command Output The **jitc show** command displays the following information.

Output field	Description
JITC mode	Displays the status of the JITC mode.
SSH AES-CTR mode	Displays the status of the SSH AES-CTR mode.
SSH AES-CBC mode	Displays the status of the SSH AES-CBC mode.

Examples The following example shows the output of the **jitc show** command.

```
device(config)#jitc show
JITC mode : Enabled
Management Protocol Specific:
SSH AES-CTR mode : Enabled
SSH AES-CBC mode : Disabled
```

History

Release version	Command history
08.0.20a	This command was introduced.

Commands A - E

aaa authorization coa enable

Enables RADIUS Change of Authorization (CoA).

Syntax **aaa authorization coa enable**

no aaa authorization coa enable

Command Default RADIUS CoA is not enabled.

Parameters None

Modes Global configuration mode

Usage Guidelines Use this command to enable RADIUS CoA authorization. The no form of the command disables the CoA functionality. A change of authorization request packet can be sent by the Dynamic Authorization Client (DAC) to change the session authorizations on the Network Access Server (NAS). This is used to change the filters, such as Layer 3 ACLs.

Before RFC 5176 when a user or device was authenticated on the RADIUS server, the session could only be ended if the user or device logs out. RFC 5176 addresses this issue by adding two more packet types to the current RADIUS standard: Disconnect Message and Change of Authorization. The Dynamic Authorization Client (DAC) server makes the requests to either delete the previously established sessions or replace the previous configuration or policies. Currently, these new extensions can be used to dynamically terminate or authorize sessions that are authenticated through multi-device-port-authentication or dot1x authentication.

Examples The following example enables RADIUS CoA.

```
device(config)# aaa authorization coa enable
```

History

Release version	Command history
08.0.20	This command was introduced.

aaa authorization coa ignore

Discards the specified RADIUS Change of Authorization (CoA) messages.

Syntax **aaa authorization coa ignore** { **dm-request** | **modify-acl** }

no aaa authorization coa ignore { **dm-request** | **modify-acl** }

Command Default The default state is maintained and the packets are not discarded.

Parameters

dm-request

Disconnects the message request.

modify-acl

Modifies the access control list.

Modes Global configuration mode

Usage Guidelines Use this command to discard the specified RADIUS messages. A CoA request packet can be sent by the Dynamic Authorization Client (DAC) to change the session authorizations on the Network Access Server (NAS). This is used to change the filters, such as Layer 3 ACLs.

Before RFC 5176 when a user or device was authenticated on the RADIUS server, the session could only be ended if the user or device logs out. RFC 5176 addresses this issue by adding two more packet types to the current RADIUS standard: Disconnect Message and Change of Authorization. The Dynamic Authorization Client (DAC) server makes the requests to either delete the previously established sessions or replace the previous configuration or policies. Currently, these new extensions can be used to dynamically terminate or authorize sessions that are authenticated through multi-device-port-authentication or dot1x authentication.

The **no** form of the command honors the dm-request message.

Examples The following example ignores the disconnect message request.

```
device(config)# aaa authorization coa ignore dm-request
```

History

Release version	Command history
08.0.20	This command was introduced.

accept-mode

Enables a non-owner master router to respond to ping, traceroute, and Telnet packets destined for the virtual IPv4 or IPv6 address of a VRRP session.

Syntax **accept-mode**

no accept-mode

Command Default A VRRP non-owner master router does not respond to any packet destined for the virtual IPv4 or IPv6 address.

Modes VRRP configuration mode

Usage Guidelines The **no** form of this command causes the non-owner master router to not respond to any packet destined for the virtual IPv4 or IPv6 address of the VRRP session.

A VRRP non-owner master router does not respond to any packet destined for the virtual IPv4 or IPv6 address. This prevents troubleshooting of network connections to this router using ping, traceroute, or Telnet. To resolve this, you can use this command to enable this router to respond to ping, traceroute, and Telnet packets destined for the virtual IPv4 or IPv6 address of a VRRP cluster. The router drops all other packets destined for the virtual IPv4 or IPv6 address of the VRRP session.

NOTE
The **accept-mode** command enables the device to respond to ping, traceroute, and Telnet packets, but the device will not respond to ssh packets.

Examples The following example shows the configuration of accept mode on an IPv6 VRRP backup router.

```
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv6 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# backup
Brocade(config-vif-3-vrid-2)# advertise backup
Brocade(config-vif-3-vrid-2)# ipv6-address 2001:DB8::1
Brocade(config-vif-3-vrid-2)# accept-mode
Brocade(config-vif-3-vrid-2)# activate
```

History

Release version	Command history
8.0.01	This command was introduced.
8.0.30b	This command was modified.

access-list enable accounting

Enables Access Control List (ACL) accounting for IPv4 numbered ACLs.

Syntax **access-list** *number* **enable-accounting**

no access-list *number* **enable-accounting**

Command Default This option is disabled.

Parameters *number*

Defines the IPv4 ACL ID.

enable-accounting

Enables ACL accounting on the specified interface.

Modes Global configuration mode

Usage Guidelines This command is only applicable to numbered ACLs.

The **no** form of this command disables ACL accounting for IPv4 numbered ACLs.

Examples The following example enables ACL accounting for a numbered ACL.

```
device(config)# access-list 10 permit host 10.10.10.1
device(config)# access-list 10 enable-accounting
device(config)# interface ethernet 1/1
device(config-if-1/1)# ip access-group 10 in
```

The following example enables ACL accounting for an extended ACL.

```
device(config)# ip access-list extended 101
device(config-ip-access-list-101)# enable-accounting
```

History

Release version	Command history
08.0.10	This command was introduced.

acl-logging

Enables logging of entries in the syslog for packets that are denied by ACL filters.

Syntax **acl-logging**

no acl-logging

Command Default ACL logging is disabled by default.

Modes Interface configuration mode

Usage Guidelines Brocade devices support ACL logging of inbound packets that are sent to the CPU for processing (denied packets). ACL logging is not supported for outbound packets or any packets that are processed in hardware (permitted packets).

When you enable logging for ACL entries, statistics for packets that match the deny conditions of the ACL entries are logged. For example, if you configure a standard ACL entry to deny all packets from source address 10.157.22.26, statistics for packets that are explicitly denied by the ACL entry are logged in the Syslog buffer and in SNMP traps sent by the device.

You can enable ACL logging on physical and virtual interfaces.

ACL logging is not supported for dynamic ACLs with MAC authentication or 802.1X enabled.

NOTE
The **acl-logging** command is applicable to IPv4 devices only. For IPv6 devices, use the **logging-enable** command.

The **no** form of the command disables ACL logging.

Examples The following example displays an ACL logging configuration on an IPv4 device.

```
device(config)# access-list 1 deny host 10.157.22.26 log
device(config)# access-list 1 deny 10.157.29.12 log
device(config)# access-list 1 deny host IPHost1 log
device(config)# access-list 1 permit any
device(config)# interface e 1/1/4
device(config-if-e1000-1/1/4)# acl-logging
device(config-if-e1000-1/1/4)# ip access-group 1 in
```

alias

An alias serves as a shorthand version of a longer CLI command.

Syntax **alias**

alias *alias-name* **=** *cli-command*

no alias *alias-name*

unalias *alias-name*

Command Default No aliases are defined.

Parameters *alias-name*

Alias name. Must be a single word, without spaces.

=

Operator representing "equals."

cli-command

Command string for which the alias is created.

Modes Privileged EXEC mode.

Global configuration mode.

Usage Guidelines To remove an alias you can enter the **no alias** or the **unalias** command followed by the *alias-name*.

An alias saves typing in a longer command that you commonly use. For example, you can create an alias called *shoro* for the CLI command **show ip route**. Then when you enter *shoro* at the command prompt, the **show ip route** command is issued.

Entering the **alias** command with no parameters displays the currently configured aliases on the device.

Examples The following example creates an alias called *shoro* for the CLI command **show ip route**, enter the **alias shoro = show ip route** command:

```
device(config)# alias shoro = show ip route
```

The following example uses the command **copy running-config** with the appropriate parameters to create an alias called *wrsbc*:

```
device(config)# alias wrsbc = copy running-config tftp 10.10.10.10 test.cfg
```

The following example removes the *wrsbc* alias from the configuration:

```
device(config)# no alias wrsbc
```

An alternate method of removing the alias is shown below:

```
device(config)# unalias wrsbc
```

To display the aliases currently configured on the Brocade device, enter the following command at either the Privileged EXEC or global configuration modes of the CLI.

```
device# alias
          wrsbc      copy running-config tftp 10.10.10.10 test.cfg
          shoro       show ip route
```

anycast-rp

Configures PIM anycast rendezvous points (RPs) in IPv4 and IPv6 multicast domains.

Syntax **anycast-rp** *rp-address anycast-rp-set-acl*

no anycast-rp *rp-address anycast-rp-set-acl*

Command Default PIM anycast RPs are not configured.

Parameters *rp-address*

Specifies a shared RP address used among multiple PIM routers.

anycast-rp-set-acl

Specifies a host-based simple access -control list (ACL) used to specify the address of the anycast RP set, including a local address.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command removes the anycast RP configuration.

PIM anycast RP is a way provide load balancing and fast convergence to PIM RPs in an IPv4 or IPv6 multicast domain. The RP address of the anycast RP is a shared address used among multiple PIM routers, known as PIM RP.

The PIM software supports up to eight PIM anycast RP routers. All deny statements in the my-anycast-rp-set-acl ACL are ignored.

Examples This example shows how to configure a PIM anycast RP.

```
Device(config)# router pim
Device(config-pim-router)#rp-address 100.1.1.1
Device(config-pim-router)#anycast-rp 100.1.1.1 my-anycast-rp-set-acl
```

This example shows how to configure PIM anycast RP 100.1.1.1.The example avoids using loopback 1 interface when configuring PIM Anycast RP because the loopback 1 address could be used as a router-id. A PIM first-hop router registers the source with the closest RP. The first RP that receives the register re-encapsulates the register to all other anycast RP peers.

```
Device(config)# interface loopback 2
Device(config-lbif-2)#ip address 100.1.1.1/24
Device(config-lbif-2)#ip pim-sparse
Device(config-lbif-2)#interface loopback 3
Device(config-lbif-3)#ip address 1.1.1.1/24
Device(config-lbif-3)#ip pim-sparse
Device(config-lbif-3)#router pim
Device(config-pim-router)#rp-address 100.1.1.1
Device(config-pim-router)#anycast-rp 100.1.1.1 my-anycast-rp-set
Device(config-pim-router)#ip access-list standard my-anycast-rp-set
Device(config-std-nacl)#permit host 1.1.1.1
Device(config-std-nacl)#permit host 2.2.2.2
Device(config-std-nacl)#permit host 3.3.3.
```

This example shows how to configure a PIM anycast RP for a VRF.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# rp-address 1001::1
Device(config-ipv6-pim-router-vrf-blue)# anycast-rp 1001::1 my-anycast-rp-set-acl
```

This example shows how to configure PIM anycast RP 1001:1 so that it avoids using loopback 1.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ipv6 address 1001::1/96
Device(config-lbif-2)# ipv6 pim-sparse
Device(config-lbif-2)# interface loopback 3
Device(config-lbif-3)# ipv6 address 1:1:1::1/96
Device(config-lbif-3)# ipv6 pim-sparse
Device(config-lbif-3)# ipv6 router pim
Device(config-ipv6-pim-router)# rp-address 1001::1
Device(config-ipv6-pim-router)# anycast-rp 1001::1 my-anycast-rp-set
Device(config-ipv6-pim-router)# ipv6 access-list my-anycast-rp-set
Device(config-std-nacl)# permit ipv6 host 1:1:1::1 any
Device(config-std-nacl)# permit ipv6 host 2:2:2::2 any
Device(config-std-nacl)# permit ipv6 host 3:3:3::3 any
```

arp-internal-priority

Configures the priority of ingress ARP packets.

Syntax **arp-internal-priority** *priority-value*

Command Default The default priority of ingress ARP packets is 4.

Parameters *priority-value*

Specifies the priority value of the ingress ARP packets. It can take a value in the inclusive range of 0 to 7, where 7 is the highest priority.

Modes Global configuration mode

Usage Guidelines High traffic volume or non-ARP packets with a higher priority may cause ARP packets to be dropped, thus causing devices to become temporarily unreachable. You can use this command to increase the priority of ingress ARP packets. However, if the priority of ARP traffic is increased, a high volume of ARP traffic might cause drops in control traffic, possibly causing traffic loops in the network.

Stacking packets have a priority value of 7 and have higher precedence over ARP packets. If the ARP packets have priority value 7 in a stack system, they will be treated as priority value 6 packets when compared to stacking packets.

This command does not affect the priority of egress ARP packets.

You cannot change the priority of ingress ARP packets on the management port.

Examples The following example sets the priority of ingress ARP packets to a value of 7.

```
Brocade(config)# arp-internal-priority 7
```

History

Release version	Command history
FastIron 08.0.01	This command was introduced.

authentication

Enters the authentication mode.

Syntax **authentication**

no authentication

Command Default Authentication mode is not enabled.

Modes Global configuration mode

Usage Guidelines The **no** form of the command will disable the authentication functionality.

Use this command to enter the authentication mode from global configuration mode. After entering authentication mode, you can configure additional authentication functionality that applies globally. Authentication functionality is also available for configuration at the interface configuration mode using different commands that apply only to the specified interface.

Examples The following example enables authentication.

```
device(config)#authentication
device(config-authen)#
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication auth-default-vlan

Specifies the default VLAN ID in interface configuration mode.

Syntax **authentication auth-default-vlan** *vlan-id*

no authentication auth-default-vlan *vlan-id*

Command Default The default VLAN is not specified.

Parameters *vlan-id*

Specifies the VLAN ID of the default VLAN.

Modes Interface configuration

Usage Guidelines The **no** form of the command disables the default VLAN.

The **authentication auth-default-vlan** command must be enabled before enabling dot1x or MAC-authentication. When any port is enabled for dot1x or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member.

Examples The following example creates a default VLAN with VLAN 3 at the interface level.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication auth-default-vlan 3
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication auth-order

Specifies the order of authentication methods, 802.1x (dot1x) and MAC authentication, at the interface level.

Syntax **authentication auth-order** {**dot1x mac-auth** | **mac-auth dot1x** }

no authentication auth-order {**dot1x mac-auth** | **mac-auth dot1x** }

Command Default The authentication order is not configured.

Parameters

dot1x mac-auth

Specifies dot1x authentication followed by MAC authentication as the order of authentication methods on the interface.

mac-auth dot1x

Specifies MAC authentication followed by dot1x authentication as the order of authentication methods on the interface.

Modes Interface configuration mode.

Usage Guidelines The **no** form of the command disables the authentication order functionality.

The **authentication auth-order** command entered at the interface level overrides the global configuration commands, **auth-order dot1x mac-auth** and **auth-order mac-auth dot1x**.

Examples The following example specifies dot1x authentication followed by MAC authentication as the order of authentication methods on Ethernet interface 1/1/3.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/3
device(config-if-e1/1/3)# authentication auth-order dot1x mac-auth
```

The following example specifies MAC authentication followed by dot1x authentication as the order of authentication methods on Ethernet interface 1/1/3.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/3
device(config-if-e1/1/3)# authentication auth-order mac-auth dot1x
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication disable-aging

Disables aging of MAC sessions at the interface level.

Syntax **authentication disable-aging** { **permitted-mac** | **denied-mac** }

no authentication disable-aging { **permitted-mac** | **denied-mac** }

Command Default Aging of MAC sessions is not disabled.

Parameters

permitted-mac

Prevents permitted (authenticated and restricted) sessions from being aged out and ages denied sessions.

denied-mac

Prevents denied sessions from being aged out, but ages out permitted sessions.

Modes Interface configuration mode

Usage Guidelines The **no** form of the command does not disable aging.

Use this command to disable the aging of MAC sessions. Use the **authentication disable-aging** command at the interface level and the **disable-aging** command in the authentication configuration mode. Entered at the interface level, this command overrides the command entered at the authentication configuration level.

Examples The following example disables aging for permitted MAC addresses.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication disable-aging denied-mac
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication dos-protection

Enables denial of service (DoS) authentication protection on the interface.

Syntax **authentication dos-protection** *mac-limit*

no authentication dos-protection *mac-limit*

Command Default Denial of service is disabled by default.

Parameters *mac-limit*

Specifies the rate limit for dos protection. You can specify a rate from 1 - 65535 authentication attempts per second. The default is a rate of 512 authentication attempts per second.

Modes Interface configuration mode

Usage Guidelines The **no** form of the command disables DoS protection.

To limit the susceptibility of the Brocade device to DoS attacks, you can configure the device to use multiple RADIUS servers, which can share the load when there are a large number of MAC addresses that need to be authenticated. The Brocade device can run a maximum of 10 RADIUS clients per server and will attempt to authenticate with a new RADIUS server if current one times out.

In addition, you can configure the Brocade device to limit the rate of authentication attempts sent to the RADIUS server. When the multi-device port authentication feature is enabled, the number of RADIUS authentication attempts made per second is tracked. When you also enable the DoS protection feature, if the number of RADIUS authentication attempts for MAC addresses learned on an interface per second exceeds a configurable rate (by default 512 authentication attempts per second), the device considers this a possible DoS attack and disables the port. You must then manually re-enable the port.

Examples The example specifies the DoS protection count as 256.

```
device(config)# authentication
device(config-authen)# interface ethernet 3/1
device(config-if-e1000-3/1)# authentication dos-protection mac-limit 256
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication fail-action

Specifies the action to be performed after a MAC or dot1x authentication failure at the interface.

Syntax **authentication fail-action** *restricted-vlan id*

no authentication fail-action *restricted-vlan id*

Command Default The default action is to block MAC addresses.

Parameters *restricted-vlan id*

Specifies the ID of the restricted VLAN.

Modes Interface configuration mode

Usage Guidelines The **no** form of the command disables the authentication failure action.

If you configure the authentication failure action to place the client port in a restricted VLAN, you can specify the ID of the restricted VLAN. If you do not specify a VLAN ID, the default VLAN is used. If a previous authentication failed, and as a result the port was placed in the restricted VLAN, but a subsequent authentication attempt was successful, the RADIUS Access-Accept message may specify a VLAN for the port. The device moves the port out of the restricted VLAN and into the RADIUS specified VLAN. If a previous authentication was successful and the RADIUS Access-Accept message specifies a VLAN for the port and then the device moves into the RADIUS-specified VLAN, but a subsequent authentication failed, the port will not be placed in the restricted VLAN. But the non-authenticated client will be blocked.

Examples The example specifies a restricted VLAN 1 for the authentication failure action.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# auth-fail-action restricted-vlan 1
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication filter-strict-security

Enables or disables strict filter security for dot1x and MAC-authentication on the interface.

Syntax **authentication filter-strict-security**

no authentication filter-strict-security

Command Default Strict filter security is not enabled.

Modes Interface configuration

Usage Guidelines The **no** form of the command disables strict filter security.

When enabled, if the filters contain invalid information, the authentication fails.

Examples The following example enables strict filter security.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication filter-strict-security
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication max-sessions

Specifies the maximum number of authenticated MAC sessions for MAC authentication and 802.1x (dot1x) authentication.

Syntax **authentication max-sessions** *count*

no authentication max-sessions *count*

Command Default The default maximum number of MAC sessions is 10.

Parameters *count*

Specifies the maximum number of authenticated MAC sessions; a value from 1 through 32.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command disables this functionality. This command is not supported on the FastIron ICX 7450 and ICX 7750 devices.

Examples The example specifies the maximum number of authenticated MAC sessions.

```
device(config)# authentication
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# auth max-sessions 30
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication reauth-timeout

Sets the time to re-authenticate a client after a timeout-action has been applied. This command is applicable for MAC authentication and dot1x authentication.

Syntax **authentication reauth-timeout** *seconds*

no authentication reauth-timeout *seconds*

Command Default The default re-authentication timeout is 60 seconds.

Parameters *seconds*

Sets the re-authentication timeout, in seconds. The range is from 60 to 4294967295.

Modes Interface configuration.

Usage Guidelines The **no** form disables re-authentication timeout.

Use this command to specify an authentication timeout action for MAC authentication or dot1x authentication enabled clients. This command sets the re-authentication timeout at the interface level after the timeout action is specified as success, restricted VLAN or critical VLAN.

Examples The example shows specifying a re-authentication timeout of 100 seconds.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/2
device(config-if-e1000-1/1/1)# authentication reauth-timeout 100
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication source-guard-protection enable

Enables Source Guard Protection along with authentication on a specified interface.

Syntax **authentication source-guard-protection enable**

no authentication source-guard-protection enable

Command Default Source Guard Protection is not enabled.

Modes Interface configuration mode

Usage Guidelines The **no** form of the command disables source guard protection.

When a new MAC session begins on a port that has Source Guard Protection enabled, the session either applies a dynamically created Source Guard ACL entry or it uses the dynamic IP ACL assigned by the RADIUS server. If a dynamic IP ACL is not assigned, the session uses the Source Guard ACL entry. The Source Guard ACL entry is **permit ip** *secure-ip* **any**, where *secure-ip* is obtained from the ARP Inspection table or from the DHCP Secure table. The DHCP Secure table is comprised of DHCP Snooping and Static ARP Inspection entries. The Source Guard ACL permit entry is added to the hardware table after all of the following events occur:

- The MAC address is authenticated
- The IP address is learned
- The MAC-to-IP mapping is checked against the Static ARP Inspection table or the DHCP Secure table

The Source Guard ACL entry is not written to the running configuration file. However, you can view the configuration using the **show auth-mac-addresses authorized-mac** command.

NOTE

The secure MAC-to-IP mapping is assigned at the time of authentication and remains in effect as long as the MAC session is active. The existing MAC session doesn't get affected if the DHCP Secure table is updated after the session is authenticated and while the session is still active.

The Source Guard ACL permit entry is removed when the MAC session expires or is cleared.

Examples The following example enables source guard protection on an interface.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication source-guard-protection enable
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication timeout-action

Specifies the action for the RADIUS server if an authentication timeout occurs.

Syntax **authentication timeout-action** { **success** | **failure** | **critical-vlan** }

no authentication timeout-action { **success** | **failure** | **critical-vlan** }

Command Default The default action is failure.

Parameters

success

Specifies the RADIUS timeout action as a success. After the successful timeout action is enabled, use the **no** form of the command to set the RADIUS timeout behavior to retry.

failure

Specifies the RADIUS timeout action as failure. Once the failure timeout action is enabled, use the **no** form of the command to reset the RADIUS timeout behavior to retry.

critical-vlan

Specifies the RADIUS timeout action as critical-VLAN. This command applies only to data traffic.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command will disable this functionality.

Examples The following example sets the **authentication timeout-action** command to success.

```
device(config)# authentication
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication timeout-action success
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-default-vlan

Specifies the default VLAN globally.

Syntax **auth-default-vlan** *vlan-id*

no auth-default-vlan *vlan-id*

Command Default The default VLAN is not specified.

Parameters *vlan-id*

Specifies the VLAN ID of the default VLAN.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables the default VLAN.

The **auth-default-vlan** command must be enabled before enabling dot1x or MAC-authentication. When any port is enabled for dot1x or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member.

Examples The following example creates a default VLAN with VLAN 2 at the authentication configuration mode.

```
device(config)# authentication
device(config-authen)# auth-default-vlan 2
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-fail-action

Specifies the authentication failure action as a restricted VLAN for both MAC authentication and dot1x authentication globally.

Syntax **auth-fail-action** *restricted-vlan id*

no auth-fail-action *restricted-vlan id*

Command Default The default action is to block MAC addresses.

Parameters *restricted-vlan id*

Specifies the ID of the restricted VLAN.

Modes Authentication mode

Usage Guidelines The **no** form of this command disables the authentication failure action.

If you configure the authentication failure action to place the client port in a restricted VLAN, you can specify the ID of the restricted VLAN. If you do not specify a VLAN ID, the default VLAN is used. If a previous authentication failed, and as a result the port was placed in the restricted VLAN, but a subsequent authentication attempt was successful, the RADIUS Access-Accept message may specify a VLAN for the port. The device moves the port out of the restricted VLAN and into the RADIUS specified VLAN. If a previous authentication was successful and the RADIUS Access-Accept message specifies a VLAN for the port and then the device moves into the RADIUS-specified VLAN, but a subsequent authentication failed, the port will not be placed in the restricted VLAN. But the non-authenticated client will be blocked.

Examples The following example specifies restricted VLAN 1 for the authentication failure action.

```
device(config)# authentication
device(config-authen)# auth-fail-action restricted-vlan 1
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-order dot1x mac-auth

Specifies the order of authentication methods to be 802.1x (dot1x) authentication before MAC authentication at the global level.

Syntax **auth-order dot1x mac-auth**

no auth-order dot1x mac-auth

Command Default The authentication order is not configured.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables the authentication order functionality.

This command specifies the dot1x authentication followed by mac authentication as the order of authentication methods on the device. Use the **auth-order mac-auth dot1x** command to reverse this order of authentication.

Examples The following example specifies dot1x authentication followed by mac authentication as the order of authentication methods.

```
device(config)# authentication
device(config-authen)# auth-order dot1x mac-auth
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-order mac-auth dot1x

Specifies the order of authentication methods to be MAC authentication before 802.1x (dot1x) authentication at the global level.

Syntax **auth-order mac-auth dot1x**

no auth-order mac-auth dot1x

Command Default The authentication order is not configured.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables the authentication order functionality.

This command specifies the MAC authentication followed by dot1x authentication as the order of authentication methods on the device. Use the **auth-order dot1x mac-auth** command to reverse this order of authentication.

Examples The following example specifies MAC authentication followed by dot1x authentication as the order of authentication methods.

```
device(config)# authentication
device(config-authen)# auth-order mac-auth dot1x
```

History

Release version	Command history
08.0.20	This command was introduced.

bsr-candidate

Configures a bootstrap router (BSR) as a candidate to distribute rendezvous point (RP) information to the other PIM Sparse devices within a PIM Sparse domain.

Syntax **bsr-candidate ethernet** *stackid/slot/portnum hash-mask-length* [*priority*]

bsr-candidate loopback *num hash-mask-length* [*priority*]

bsr-candidate ve *num hash-mask-length* [*priority*]

bsr-candidate tunnel *num hash-mask-length* [*priority*]

no bsr-candidate

Command Default The PIM router does not participate in BSR election.

Parameters **ethernet** *stackid/slot/portnum*

Specifies the physical interface for the candidate BSR. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *num*

Specifies the loopback interface for the candidate BSR.

ve *num*

Specifies the virtual interface for the candidate BSR.

tunnel *num*

Specifies a GRE tunnel interface.

hash-mask-length

Specifies the number of bits in a group address that are significant when calculating the group-to-RP mapping. The range is 1 to 32.

NOTE
It is recommended that you specify 30 for IPv4 networks.

priority

Specifies the BSR priority. The range is from 0 to 255, from low to high. The default is 0.

Modes Router configuration mode

Usage Guidelines The **no** form of this command makes the PIM router cease to act as a candidate BSR.

Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority is elected. If the priorities result in a tie, the candidate BSR interface with the highest IP address is elected.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

Examples The following example uses a physical interface to configure a device as a candidate BSR.

```
Device(config)# router pim
Device(config-pim-router)# bsr-candidate ethernet 2/2 30 255
```

The following example uses a loopback interface to configure a device as a candidate BSR.

```
Device(config)# router pim
Device(config-pim-router)# bsr-candidate loopback 1 30 240
```

The following example uses a virtual interface to configure a device as a candidate BSR.

```
Device(config)# router pim
Device(config-pim-router)# bsr-candidate ve 120 30 250
```

History

Release version	Command history
8.0.20	This command was modified to add the **tunnel** keyword.

clear access-list accounting

Clears Access Control List (ACL) accounting statistics for IPv4 ACLs, IPv6 ACLs, and Layer 2 MAC filters.

Syntax **clear access-list accounting all**

clear access-list accounting *interface-type interface-name* **in**

clear access-list accounting traffic-policy { **all** | *name* }

Parameters **all**

Clears all statistics for all ACLs.

interface-type interface-name

Specifies the ID of the Ethernet or virtual interface. Clears the accounting statistics for ACLs bound to a physical port or clears statistics for all ACLs bound to ports that are members of a virtual routing interface.

in

Clears statistics of the inbound ACLs.

traffic-policy

Clears traffic-policy statistics.

all

Clears all traffic-policy statistics.

name

Clears statistics of a specific traffic-policy.

Modes Privileged EXEC mode

Usage Guidelines To clear accounting statistics for all configured ACLs, use the **all** keyword.

Examples The following example clears ACL accounting statistics for all configured ACLs.

```
device# clear access-list accounting all
```

The following example clears ACL accounting statistics for a specific port.

```
device# clear access-list accounting ethernet 1/5 in
```

The following example clears all traffic-policy statistics.

```
device#clear access-list accounting traffic-policy all
```

History

Release version	Command history
08.0.10	This command was introduced.

clear cable diagnostics tdr

Clears the results of Virtual Cable Test (VCT) TDR testing (if any) conducted on the specified port

Syntax **clear cable-diagnostics tdr** *stackid/slot/port*

Command Default By default, the results of the previous test (if any) are present and are displayed in response to the **show cable-diagnostics tdr** command for the specified port.

Parameters *stackid/slot/port*

Identifies the specific interface (port), by device, slot, and port number in the format shown.

Modes Privileged EXEC mode

Usage Guidelines Use this command to clear TDR test registers before every TDR cable diagnostic test. Most Brocade devices support VCT technology. VCT technology enables the diagnosis of a conductor (wire or cable) by sending a pulsed signal into the conductor, then examining the reflection of that pulse. This method of cable analysis is referred to as Time Domain Reflectometry (TDR). By examining the reflection, the Brocade device can detect and report cable statistics such as local and remote link pair, cable length, and link status.

Use the command in conjunction with the **phy cable-diagnostics tdr stackid/slot/port** command to test the interface.

Show diagnostic test results using the **show cable-diagnostics tdr stackid/slot/port** command.

This command is supported only on the Brocade ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, ICX6450-C, and FCX Series devices.

Examples In the following example, results from the previous test are cleared from the third interface on the second slot of the first device in the stack.

```
device# clear cable-diagnostics tdr 1/2/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear dot1x sessions

Clears 802.1x (dot1x) authentication sessions.

Syntax **clear dot1x sessions** { *mac-address* | **ethernet** *deviceIslotIport* }

Parameters *mac-address*

Specifies the mac-address from which the dot1x authentication sessions are to be cleared.

ethernet *deviceIslotIport*

Specifies the interface from which the dot1x authentication sessions are to be cleared.

Modes Privileged EXEC mode.

Usage Guidelines Use this command to clear the dot1x authentication sessions.

Examples The following example clears the dot1x authentication session for the specified MAC address.

```
device(config)# clear dot1x sessions 0000.0034.abd4
```

History

Release version	Command history
08.0.20	This command was introduced.

clear dot1x statistics

Clears dot1x authentication statistics.

Syntax **clear dot1x statistics** { **ethernet** *device*/*slot*/*port* | **all** }

Parameters

ethernet *device*/*slot*/*port*

Specifies the interface on which the dot1x authentication statistics are to be cleared.

all

Specifies that dot1x authentication statistics are to be cleared for all interfaces.

Modes Privileged EXEC mode.

Usage Guidelines Use this command to clear dot1x authentication statistics on all or one specified interface.

Examples The following example clears dot1x statistics on all interfaces.

```
device(config)# clear dot1x statistics all
```

History

Release version	Command history
08.0.20	This command was introduced.

clear dot1x-mka statistics

Clears current MACsec Key Agreement (MKA) statistics.

Syntax **clear dot1x-mka statistics ethernet** *device*/*slot*/*port*

Parameters **ethernet** *device*/*slot*/*port*

Specifies an Ethernet interface by device position in stack, slot on the device, and interface on the slot.

Modes EXEC or Privileged EXEC mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

Examples In the following example, MKA statistics are cleared for Ethernet interface 1/3/3 (port 3 of slot 3 on the first device in the stack).

```
device# clear dot1x-mka statistics ethernet 1/3/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear ip mroute

Removes multicast routes from the IP multicast routing table .

Syntax **clear ip mroute** [**vrf** *vrf-name*] [*ip-address* {*ip-mask* | *mask-bits* }]

Parameters

vrf *vrf-name*
: Specifies a VRF.

ip-address
: Specifies an IP address.

ip-mask
: Specifies an IP subnet mask.

mask-bits
: Specifies a subnet mask in bits.

Modes Global configuration mode

Usage Guidelines After multicast routes are cleared from an IP multicast routing table, the best static multicast routes are added back to the routing table.

When used without specifying a **vrf** *vrf-name* this command clears multicast routes from the multicast routing table.

Examples The following example removes all mroutes from the IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute
```

The following example removes all mroutes from the vrf green IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute vrf green
```

The following example removes mroute 10.0.0.2/24 from the IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute 10.0.0.2/24
```

History

Release version	Command history
8.0.10a	This command was introduced.

clear ip pim counters

Clears PIM message counters.

Syntax **clear ip pim** [**vrf** *vrf-name*] **counters**

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

counters

Specifies PIM message counters.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears the PIM message counters for all VRFs.

Examples The following example clears the PIM message counters.

```
Device# clear ip pim counters
```

The following example clears the PIM message counters on a XRF named blue.

```
Device# clear ip pim vrf blue counters
```

clear ip pim hw-resource

Clears the PIM hardware resource fail count for a specific VRF instance or for all VRFs.

Syntax **clear ip pim** [**vrf** *vrf-name*] **hw-resource**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

hw-resource

Specifies hardware resource fail count.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears the PIM hardware resource fail count for all VRFs.

Examples The following example clears the PIM hardware resource fail count.

```
Device# clear ip pim hw-resource
```

clear ip pim rp-map

Updates the entries in the static multicast forwarding table for a specific VRF instance or for all VRFs.

Syntax **clear ip pim** [**vrf** *vrf-name*] **rp-map**

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

rp-map

Specifies the entries in a PIM sparse static multicast forwarding table.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears the PIM forwarding cache for all VRFs.

Configure this command to update the entries in the static multicast forwarding table immediately after making rendezvous point (RP) configuration changes. This command is meant to be used with the **rp-address** command.

Examples The following example clears the entries in a PIM sparse static multicast forwarding table on a VRF instance named blue.

```
Device# clear ip pim vrf blue rp-map
```

clear ip pimsm-snoop

Clears PIM sparse mode (SM) information.

Syntax **clear ip pimsm-snoop** [**vlan***vlan-id*] { **cache** [*ip-address*] | **stats**}

Parameters

vlan*vlan-id*
Specifies clearing information on a specific VLAN.

cache
Specifies clearing the PIM SM snooping cache.

ip-address
Specifies clearing PIM SM snooping-cache information on a specific source or group.

stats
Specifies clearing traffic and error counters.

Modes Global configuration mode

Examples The following example clears PIM SM information from all VLANs.

```
Device(config)#clear ip pimsm-snoop cache
```

The following example clears PIM SM information from a specific VLAN.

```
Device(config)#clear ip pimsm-snoop vlan 10 cache
```

The following example clears PIM SM information from a specific source.

```
Device(config)#clear ip pimsm-snoop cache 10.1.1.1
```

The following example clears traffic and error counters from all VLANs.

```
Device(config)#clear ip pimsm-snoop stats
```

History

Release version	Command history
8.0.20	This command was introduced.

clear ipv6 mroute

Removes IPv6 multicast routes from the IPv6 multicast routing table.

Syntax **clear ipv6 mroute** [**vrf** *vrf-name*] [*ipv6-address-prefix/prefix-length*]

Parameters **vrf** *vrf-name*

Specifies a VRF route.

ipv6-address-prefix/prefix-length

Specifies an IPv6 address prefix in hexadecimal using 16-bit values between colons as documented in RFC 2373 and a prefix length as a decimal value.

Modes Privileged EXEC mode

Usage Guidelines After mroutes are removed from an IPv6 multicast routing table, the best static mroutes are added back to it.

Examples The following example removes all mroutes from the IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute
```

The following example removes all mroutes from the vrf green IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute vrf green
```

The following example removes mroute 2000:7838::/32 from the IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute 2000:7838::/32
```

History

Release version	Command history
8.0.10a	This command was introduced.

clear ipv6 neighbor

Clears the static neighbor discovery (ND) inspect entries and ND inspection statistics.

Syntax **clear ipv6 neighbor** [**vrf** *vrf-name*] **inspection** [**static-entry** | **statistics**]

Parameters

vrf
Specifies the VRF instance (optional).

vrf-name
Specifies the ID of the VRF instance required with **vrf** .

inspection
Specifies that the neighbor discovery messages are verified against the static ND inspection entries or dynamically learned DHCPv6 snoop entries.

static-entry
Clears the manually configured static ND inspect entries that are used to validate the packets received on untrusted ports.

statistics
Clears the total number of neighbor discovery messages received and the number of packets discarded after ND inspection.

Modes Privileged EXEC mode

Global configuration mode

VRF configuration mode

Usage Guidelines This command can be used in three different modes as shown in the examples. If used without specifying a VRF, this command clears data from the default VRF.

Examples The following example removes the manually configured static ND inspect entries.

```
device# clear ipv6 neighbor inspection static-entry
```

The following example removes the manually configured static ND inspect entries on a VRF.

```
device# configure terminal
device(config)# vrf vrf2
device(config-vrf-vrf2)# clear ipv6 neighbor vrf vrf2 inspection static-entry
```

The following example deletes the ND inspection statistics.

```
device# configure terminal
device(config)# clear ipv6 neighbor inspection statistics
```

The following example deletes the ND inspection statistics on a VRF.

```
device# configure terminal
device(config)# clear ipv6 neighbor vrf vrf2 inspection statistics
```

History

Release version	Command history
08.0.20	This command was introduced.

clear ipv6 pim cache

Clears the IPv6 PIM forwarding cache.

Syntax **clear ipv6 pim** [**vrf** *vrf-name*] **cache** *ipv6-address*

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

cache *ipv6-address*

Specifies group or address of the PIM forwarding cache to clear.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears information for all VRF instances.

Examples This example shows how to clear the IPv6 PIM forwarding cache:

```
Device#clear ipv6 pim cache 2001:0DB8:0:1::1/120 5100::192:1:1:1
```

clear ipv6 pim counters

Clears IPv6 PIM message counters.

Syntax **clear ipv6 pim** [**vrf** *vrf-name*] **counters**

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

counters

Specifies the IPv6 PIM message counters.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears information for all VRF instances.

Examples Thi example shows how to clear the IPv6 PIM message counters:

```
Device#clear ipv6 pim counters
```

clear ipv6 pim hw-resource

Clears the IPv6 PIM hardware resource fail count for a specific VRF instance or for all VRFs.

Syntax **clear ipv6 pim hw-resource**

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

hw-resource

Specifies hardware resource fail count.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears the PIM hardware resource fail count for all VRFs.

Examples The following example clears the IPv6 PIM hardware resource fail count.

```
Device# clear ipv6 pim hw-resource
```

clear ipv6 pim rp-map

Clears the entries in an IPv6 PIM Sparse static multicast forwarding table, allowing a new rendezvous point (RP) configuration to be effective immediately.

Syntax **clear ipv6 pim** [**vrf** *vrf-name*] **rp-map**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

rp-map

Specifies the entries in a PIM sparse static multicast forwarding table.

Modes Privileged EXEC mode

Usage Guidelines Configuring this command clears and overwrites the static RP configuration. If you change the static RP configuration, the entries in the IPv6 PIM Sparse multicast forwarding table continue to use the old RP configuration until they are aged out. You can configure the **clear ipv6 pim rp-map** command to update the entries in the static multicast forwarding table immediately after making RP configuration changes.

This command is meant to be used with the **rp-address** command.

Examples This example shows how to clear the entries in an IPv6 PIM Sparse static multicast forwarding table after you change the RP configuration:

```
Device#clear ipv6 pim rp-map
```

clear ipv6 pim traffic

Clears counters on IPv6 PIM traffic.

Syntax **clear ipv6 pim** [**vrf** *vrf-name*] **traffic**

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

traffic

Specifies counters on IPv6 PIM traffic.

Modes Privileged EXEC mode

Usage Guidelines When entered without the **vrf** keyword, this command clears counters for all VRF instances.

Examples This example shows how to clear IPv6 PIM traffic counters on all VRF instances:

```
Device#clear ipv6 pim traffic
```

clear ipv6 pimsm-snoop

Clears PIM sparse mode (SM) information.

Syntax **clear ipv6 pimsm-snoop** [**vlan***vlan-id*] { **cache** [*ipv6-address*] | **stats**}

Parameters

vlan*vlan-id*

Specifies clearing information on a specific VLAN.

cache

Specifies clearing the PIM SM snooping cache.

ipv6-address

Specifies clearing PIM SM snooping-cache information on a specific source or group.

stats

Specifies clearing traffic and error counters.

Modes Global configuration mode

Examples The following example clears PIM SM information from all VLANs.

```
Device(config)#clear ipv6 pimsm-snoop cache
```

The following example clears PIM SM information from a specific VLAN.

```
Device(config)#clear ipv6 pimsm-snoop vlan 10 cache
```

The following example clears PIM SM information from a specific source.

```
Device(config)#clear ipv6 pimsm-snoop cache ff05::100
```

The following example clears traffic and error counters from all VLANs.

```
Device(config)#clear ipv6 pimsm-snoop stats
```

History

Release version	Command history
8.0.20	This command was introduced.

clear ipv6 raguard

Resets the drop or permit packet counters for Router Advertisement (RA) guard policies.

Syntax **clear ipv6 raguard** { *name* | **all** }

Parameters *name*

An ASCII string indicating the name of the RA guard policy of which the packet counters must be cleared.

all

Clears the packet counters of all RA guard policies.

Modes Global configuration mode

Usage Guidelines To clear RA guard packet counters for all RA guard policies, use the **all** keyword. To clear the RA guard packet counters for a specific RA guard policy, specify the *name* of the policy.

Examples The following example clears the packet count for an RA guard policy:

```
Brocade(config)# clear ipv6 raguard policy1
```

The following example clears the packet counters for all RA guard policies:

```
Brocade(config)# clear ipv6 raguard all
```

clear macsec ethernet

Clears the MACsec traffic statistics for the specified interface.

Syntax **clear macsec ethernet** *device*/*slot*/*port*

Parameters *device*/*slot*/*port*

Specifies an interface by device position in stack, slot on the device, and interface on the slot.

Modes Privileged EXEC mode.

Usage Guidelines This command is supported only on the Brocade ICX 6610.

Examples In the following example, MACsec traffic statistics are cleared for interface 1/3/3 (port 3 of slot 3 on the first device in the stack).

```
device(config-dot1x-mka-1/3/3)# clear macsec ethernet 1/3/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear mac-authentication sessions

Clears MAC authentication sessions.

Syntax **clear mac-authentication sessions** { **mac-address** *mac-address* | **ethernet** *deviceIslotIport* }

Parameters *mac-address*

Specifies the mac-address from which the MAC authentication sessions are to be cleared.

ethernet *deviceIslotIport*

Specifies the interface from which the MAC authentication sessions are to be cleared.

Modes Privileged EXEC mode.

Usage Guidelines Use this command to clear the MAC authentication sessions for either a specified MAC address or an ethernet interface.

Examples The following example clears the MAC authentication session for the specified MAC address.

```
device# clear mac-authentication sessions 0000.0034.abd4
```

History

Release version	Command history
08.0.20	This command was introduced.

clear notification-mac statistics

Clears the MAC-notification statistics, such as the number of trap messages and number of MAC notification events sent.

Syntax **clear notification-mac statistics**

Command Default The MAC-notification statistics are available on the device.

Modes Global configuration

Privileged EXEC

Usage Guidelines MAC notification statistics can be viewed using the **show notification-mac** display command.

Examples The following example clears the MAC notification statistics:

```
device(config)# clear notification-mac statistics
```

History

Release version	Command history
08.0.10	This command was introduced.

clear openflow

Clears flows from the flow table.

Syntax **clear openflow** { **flowid** *flow-id* | **all** }

Parameters

flowid *flow-id*

Clears the given flow ID that you want to delete from the flow table.

all

Deletes all flows from the flow table.

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines When an OpenFlow rule or all flows in the flow table need to be deleted you can use the **clear openflow** command with the **all** option. To delete a single OpenFlow rule based on a flow-id, use the **clear openflow** command with the **flowid** *flow-id* options.

Examples The following example clears the flow with an ID of 6.

```
device# clear openflow flowid 6
```

The following example clears all flows in the flow table.

```
device# clear openflow all
```

History

Release	Command History
08.0.20	This command was introduced.

clear stack ipc

Clears stack traffic statistics.

Syntax **clear stack ipc**

Command Default Stack traffic statistics are collected and retained.

Modes Privileged EXEC mode

Usage Guidelines Use the **clear stack ipc** command before issuing the **show stack ipc** command. This helps to ensure that the data are the most recent traffic statistics for the stack.

This command must be executed from the active stack controller.

Examples The following example clears stack traffic statistics prior to using the **show stack ipc** command to display current stack traffic statistics.

```
device# clear stack ipc
device# show stack ipc
V15, G1, Recv: SkP0:3749372, P1:3756064, MAIL:184291175, sum:191796611, t=457152.2
Message types have callbacks:
1 :Reliable IPC message 2 :Reliable IPC atomic 4 :fragmentation, jumbo
5 :probe by mailbox 6 :rel-mailbox 7 :test ipc
8 :disable keep-alive 9 :register cache 10:ipc dnld stk
11:chassis operation 12:ipc stk boot 13:Rconsole IPC message
14:auth msg 15:ipc erase flash 16:unconfigure
17:ipc stk boot 18:ss set 19:sFlow IPC message
21:SYNC download reques 23:SYNC download 1 spec 28:SYNC client hello
30:SYNC dy chg error 32:active-uprintf 33:test auth msg
34:probe KA 39:unrel-mailbox 40:trunk-probe
Send message types:
[1]=2342639, [4]=44528, [5]=961830, [6]=37146,
[9]=73104634, [11]=137082, [14]=487007, [20]=2304,
[22]=1395, [25]=23, [26]=1901701, [29]=415888,
[34]=1827543, [39]=30451, [40]=289420,
Recv message types:
[1]=2016251, [4]=1352759, [5]=470884, 475144,
[6]=114459, 114572, [9]=367644144, [11]=1785229,
[14]=973285, 974177, [21]=1395, [30]=25,
[34]=912972, 914086, [39]=973492, 973440, [40]=700313,
Statistics:
send pkt num : 34068433, recv pkt num : 191796609,
send msg num : 79756048, recv msg num : 379902767,
send frag pkt num : 22264, recv frag pkt num : 493860,
pkt buf alloc : 34068433,
Reliable-mail send success receive duplic
target ID 1 1 0 0
target MAC 15230 15230 0 0
unrel target ID 7615 0
There is 1 current jumbo IPC session
Possible errors:
*** recv from non-exist unit 2 times: unit 5
```

History

Release version	Command history
08.0.00a	This command was introduced.

clear statistics openflow

Clears OpenFlow statistics.

Syntax **clear statistics openflow** { **group** | **meter** | **controller** }

Parameters

group

Clears statistics for all groups.

meter

Clears statistics for all meters.

controller

Clears statistics for all controllers.

Modes EXEC and Privileged EXEC mode

Global configuration mode

Usage Guidelines This command can be entered in three configuration modes as shown in the examples below.

Examples The following example, entered in User EXEC mode, clears statistics for all groups in User EXEC mode.

```
device> clear statistics openflow group
```

The following example, entered in Privileged EXEC mode, clears statistics for all meters in Privileged EXEC mode.

```
device> enable
device# clear statistics openflow meter
```

The following examples, entered in global configuration mode, clears statistics for all controllers.

```
device# configure terminal
device(config) # clear statistics openflow controller
```

History

Release	Command History
08.0.20	This command was introduced.

connect

Specifies the devices to which a peripheral device connects in a mixed stack.

Syntax **connect** *stack-unit*|*slotnum*|*portnum*

no connect *stack-unit*|*slotnum*|*portnum*

Parameters *stack-unit*

Specifies the stack unit ID.

slotnum

Specifies the slot number.

portnum

Specifies the port number in the slot. If the port is part of a trunk, specify only the first port number (the odd-numbered port) in the trunk.

Modes Stack unit configuration mode

Usage Guidelines The **connect** command can only be used on the ICX 6610.

The **no** form of this command removes the connection configuration.

The active controller always generates a connect for live peripheral units during stack construction.

This command is optional and can be specified only for peripheral units. You cannot override the physical connections using the **connect** command. However, you can use this command on peripheral devices to make sure that a peripheral device has the unit ID you want if a unit is replaced.

You can use this command when configuring a mixed stack with the automatic configuration method.

Examples The following example connects stack unit 3 (a peripheral device) to stack unit 1 (the active controller) and to stack unit 4 (another peripheral device).

```
Brocade(config-unit-3)# connect 1/3/1
Brocade(config-unit-3)# connect 4/2/3
```

History

Release	Command History
08.0.00a	This command was introduced.

copy flash scp

Uploads a copy of an OS image file from a FastIron device's primary or secondary flash memory to an SCP server. The syntax for copying an image between two devices under test (DUTs) is different from the syntax for uploading from a Brocade device to a Linux or a Windows server.

Syntax Syntax for copying an image between two DUTs:

copy flash scp { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-prefix/prefix-length* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { **flash:primary** | **secondary** }

Syntax for uploading from a Brocade device to a Linux or a Windows server:

copy flash scp { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-prefix/prefix-length* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { **primary** | **secondary** }

Parameters

ipv4-address-

Specifies the IPV4 address of the SCP server.

ipv4-hostname-

Specifies the IP hostname of the SCP server.

ipv6

Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length

Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-

Specifies the IPv6 hostname of the SCP server.

outgoing-interface

Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*

Configures an Ethernet interface as the outgoing interface.

ve *ve-number*

Configures a virtual interface (VE) as the outgoing interface.

public-key

Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa

Specifies DSA as the public key authentication.

rsa

Specifies RSA as the public key authentication.

remote-port

Specifies the remote port number for the TCP connection.

remote-filename

Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

flash:primary

Specifies the binary image in primary flash memory. Configure the **flash:primary** keyword when transferring files between DUTs,. See the usage note regarding using this keyword when transferring files between DUTs.

primary

Specifies the binary image in primary flash memory.

secondary

Specifies the binary image in secondary flash memory.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

NOTE

When transferring files between DUTs, you should configure the **flash:primary** keyword instead of the **primary** keyword because the SCP server does not support remote-filename aliases.

Examples The following example uploads a copy of an OS image file from the primary flash memory on a Brocade device to the SCP server:

```
device# copy flash scp 10.20.1.1 FCXR08011-scp.bin primary
device# copy flash scp 10.20.1.1 FCXR08011-scp.bin secondary
```

The following example uploads a copy of an OS image file from the primary flash memory on a Brocade device to an SCP server with the IP address of 172.26.51.180 :

```
device# copy flash scp 172.26.51.180 filename primary
```

The following example specifies that the SCP connection is established using SSH public key authentication:

```
device# copy flash scp 172.26.51.180 public-key dsa filename primary
```

History

Release version	Command history
08.0.20	This command was introduced.

copy running-config scp

Uploads a copy of the running configuration file from a FastIron device to an SCP server.

Syntax **copy running-config scp** { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address
Specifies the IPV4 address of the SCP server.

ipv4-hostname
Specifies the IP hostname of the SCP server.

ipv6
Specifies the IPV6 address method for SCP file transfer.

ipv6-address
Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
Specifies the IPv6 hostname of the SCP server.

outgoing-interface
Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
Configures a virtual interface (VE) as the outgoing interface.

public-key
Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
Specifies DSA as the public key authentication.

rsa
Specifies RSA as the public key authentication.

remote-port
Specifies the remote port number for the TCP connection.

remote-filename
Specifies the name of the file in the SCP server that is going to be uploaded. You can specify up to 127 characters for the filename.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

Examples The following example uploads a copy of the running configuration file from a FastIron device to a 172.26.51.180 SCP server:

```
device# copy running-config scp 172.26.51.180 runConfig
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp flash

Downloads from an SCP server a copy of the OS image file to a FastIron's device's primary or secondary flash memory or a copy of the boot file or the signature file to the FastIron device. The syntax for copying an image between two devices under test (DUTs) is different from the syntax for downloading from a DUT to a Linux or a Windows server.

Syntax

Syntax for copying an image between two DUTs:

copy scp flash { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { { **flash:primary** | **secondary** } | **bootrom** | { **fips-primary-sig** | **fips-secondary-sig** | **fips-bootrom-sig** } } [**icx6450** | **icx6610**]

Syntax for downloading from a DUT to a Linux or a Windows server:

copy scp flash { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { { **primary** | **secondary** } | **bootrom** | { **fips-primary-sig** | **fips-secondary-sig** | **fips-bootrom-sig** } } [**icx6450** | **icx6610**]

Parameters

ipv4-address

Specifies the IPV4 address of the SCP server.

ipv4-hostname

Specifies the IP hostname of the SCP server.

ipv6

Specifies the IPV6 address method for SCP file transfer.

ipv6-address

Specifies the IPV6 address of the SCP server.

ipv6-hostname

Specifies the IPv6 hostname of the SCP server.

outgoing-interface

Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*

Configures an Ethernet interface as the outgoing interface.

ve *ve-number*

Configures a virtual interface (VE) as the outgoing interface.

public-key

Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa

Specifies DSA as the public key authentication.

rsa

Specifies RSA as the public key authentication.

remote-port

Specifies the remote port number for the TCP connection.

remote-filename

Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

flash:primary

Specifies the binary image in primary flash memory. Configure the **flash:primary** keyword when transferring files between DUTs,. See the usage note regarding using this keyword when transferring files between DUTs.

primary

Specifies the binary image in primary flash memory. Configure the **primary** keyword when transferring files between DUTs. See the usage note regarding using this keyword when transferring files between DUTs.

secondary

Specifies the binary image in secondary flash memory.

bootrom

Specifies the boot file image in the SCP server.

fips-primary-sig

Specifies the signature filename in SCP server.

fips-secondary-sig

Specifies the signature filename in SCP server.

fips-bootrom-sig

Specifies the signature filename in SCP server.

icx6450

Specifies the FastIron ICX 6450 as the device to which the signature file is downloaded.

icx6610

Specifies the FastIron ICX 6610 as the device to which the signature file is downloaded.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

NOTE

When transferring files between DUTs, you should configure the **flash:primary** keyword instead of the **primary** keyword because the SCP server does not support remote-filename aliases.

Examples

The following example copies an image from an SCP server to a Brocade device:

```
device# copy scp flash 10.20.1.1 FCXR08011.bin primary
device# copy scp flash 10.20.1.1 FCXR08011.bin secondary
```

The following example downloads a copy of the signature file from a 172.26.51.180 SCP server to a Brocade ICX 6610 device:

```
device# copy scp flash 172.26.51.180 /tftpboot/ICX6610.sig fips-primary-sig
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp license

Downloads a copy of the license file from an SCP server to a FastIron device.

Syntax **copy scp license** { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid*|*slot*|*port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* [**unit** *unit-id*]

Parameters

ipv4-address-
: Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid*|*slot*|*port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the local port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

unit *unit-id*
: Specifies the unit ID of the device in the stack. If two or more pizza-box devices are connected and acting as a single device, a single management ID is assigned to the stack.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

Examples The following example downloads a copy of the license file from an SCP server to a FastIron device:

```
Device# copy scp license 172.26.21.180 /tftpboot/abc.xml unit 1
Device#
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp running-config

Downloads a copy of the running configuration file from an SCP server to a FastIron device.

Syntax **copy scp running-config** { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } [**outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* }] } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* **overwrite**

Parameters

ipv4-address
: Specifies the IPV4 address of the SCP server.

ipv4-hostname
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

overwrite
: Specifies that the FastIron device should overwrite the current configuration file with the copied file. If you do not specify the **overwrite** keyword, the device copies the downloaded file into the current running or startup configuration but does not overwrite the current configuration.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

Examples The following example downloads a copy of the running configuration file from an SCP server to a FastIron device:

```
device# copy scp running-config 172.26.51.180 abc.cfg
```

The following example downloads a copy of the running configuration file from an SCP server to a FastIron device and overwrite the current configuration file with the copied file:

```
device# copy scp running-config 172.26.51.180 abc.cfg overwrite
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp startup-config

Downloads a copy of the startup configuration file from an SCP server to a FastIron device.

Syntax **copy scp startup-config** { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address
Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname
Specifies the IP hostname of the SCP server.

ipv6
Specifies the IPV6 address method for SCP file transfer.

ipv6-address
Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
Specifies the IPv6 hostname of the SCP server.

outgoing-interface
Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
Configures a virtual interface (VE) as the outgoing interface.

public-key
Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
Specifies DSA as the public key authentication.

rsa
Specifies RSA as the public key authentication.

remote-port
Specifies the remote port number for the TCP connection.

remote-filename
Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

Examples The following example downloads a copy of the startup configuration file from an SCP server to a FastIron device:

```
device# copy scp startup-config 172.26.51.180 abc.cfg
```

History

Release version	Command history
08.0.20	This command was introduced.

copy startup-config scp

Uploads a copy of the startup configuration file from a FastIron device to an SCP server.

Syntax **copy startup-config scp** { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address-
: Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes Privileged EXEC mode

Usage Guidelines You are prompted for username and password when you configure this command.

Examples The following example uploads a copy of the startup configuration file from a FastIron device to a to a 172.26.51.180 SCP server:

```
device# copy startup-config scp 172.26.51.180 my_startup_file
```

History

Release version	Command history
08.0.20	This command was introduced.

critical-vlan

Specifies the VLAN into which the client should be placed when the RADIUS server times out while authenticating or re-authenticating users.

Syntax **critical-vlan** *vlan-id*

no critical-vlan *vlan-id*

Command Default The client is not part of the critical VLAN.

Parameters *vlan-id*

Specifies the VLAN ID of the specific critical VLAN.

Modes Authentication mode.

Usage Guidelines The **no** form of the command disables the critical VLAN by removing the client from the VLAN.

Examples The following example enables VLAN 20 as critical VLAN.

```
device(config)# authentication
device(config-authen)# critical-vlan 20
```

History

Release version	Command history
08.0.20	This command was introduced.

default-ports

Assigns ports (interfaces) other than the factory-assigned ports as the default stacking ports.

Syntax **default-ports** *unit*/*slot*/ *port*

no default-ports

Command Default The factory-assigned default stacking ports are the only default stacking ports on the device.

Parameters *unit*

Stack unit ID for the device on which the interface resides.

slot

Stack unit slot or module on which the interface resides.

port

Interface to be used as a default stacking port.

Modes Stack unit configuration mode

Usage Guidelines The **no** form of the command restores the factory-assigned default stacking ports. Any ports you previously assigned as the default stacking ports using the **default-ports** command are overwritten.

When you use the **default-ports** command, the factory-assigned default stacking ports are no longer the default stacking ports.

Only valid stacking ports can be assigned as default stacking ports. Valid ports vary depending on the type of FastIron device.

Tagged ports cannot be assigned as default stacking ports.

The number of ports you can assign as default stacking ports varies depending on the type of FastIron device. Some devices allow you to assign two ports as the default stacking ports, and some devices allow you to assign a single port as the default stacking port.

Examples The following example assigns the stacking ports on Module 3 on the rear panel of an ICX 7750 as the default stacking ports.

```
device# configure terminal
device(config)# stack unit 1
device¡(config-unit-1)# default-ports 1/3/1 1/3/4
```

disable-aging

Disables aging of MAC sessions at the global level.

Syntax **disable-aging** { **permitted-mac** | **denied-mac** }

no disable-aging { **permitted-mac** | **denied-mac** }

Command Default Aging of MAC sessions is not disabled.

Parameters

permitted-mac

Prevents permitted (authenticated and restricted) sessions from being aged out and ages denied sessions.

denied-mac

Prevents denied sessions from being aged out, but ages out permitted sessions.

Modes Authentication mode

Usage Guidelines The **no** form of the command does not disable aging.

Use this command to disable the aging of MAC sessions. Use the **disable-aging** command in the authentication mode and the **authentication disable-aging** command at the interface level. The command entered at the interface level overrides the command entered at the authentication level.

Examples The example disables aging for permitted MAC addresses.

```
device(config)# authentication
device(config-authen)# disable-aging permitted-mac
```

History

Release version	Command history
08.0.20	This command was introduced.

disable authentication md5

Disables the MD5 authentication scheme for Network Time Protocol (NTP).

Syntax **disable authentication md5**

no disable authentication md5

Command Default If JITC is enabled, the MD5 authentication scheme is disabled. In the standard mode, the MD5 authentication scheme is enabled.

Modes Global configuration mode

Usage Guidelines In the standard mode, both SHA1 and MD5 authentication schemes are supported. If JITC is enabled, The MD5 authentication for Network Time Protocol (NTP) is disabled by default and the **disable authentication md5** command can be seen in the running configuration. In the JITC mode, only the SHA1 option is available. The SHA1 authentication scheme must be enabled manually to define the authentication key for NTP using the **authentication-key key-id** command.

The **no** form of the command enables the MD5 authentication scheme.

Examples The following example disables the MD5 authentication scheme.

```
device(config)# disable authentication md5
```

History

Release version	Command history
08.0.20a	This command was introduced.

dlb-internal-trunk-hash

Changes the hashing method for inter-packet-processor (inter-pp) HiGig links that are used to connect master and slave units in ICX 7450-48 devices.

Syntax **dlb-internal-trunk-hash** { **inactivity-mode** | **spray-mode** }

no dlb-internal-trunk-hash { **inactivity-mode** | **spray-mode** }

Command Default The hashing method is inactivity mode.

Parameters

inactivity-mode

Specifies that the flow is set by the inactivity of traffic loading.

spray-mode

Specifies that the flow is set to receive new member assignments for every packet arrival in accordance with the traffic loading of each aggregate member.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default hashing method.

NOTE
This command is supported only on ICX 7450-48 devices that have master and slave units.

Dynamic load balancing (DLB) enhances hash-based load balancing by taking into account the traffic loading in the network. The inter-pp HiGig links in ICX7450-48 devices use hash-based load balancing to distribute traffic evenly. You can configure the **dlb-internal-trunk-hash** command to change the hashing method.

Examples The following example globally enables spray mode as the inter-pp links hashing method.

```
ICX7450-48P Router(config)#dlb-internal-trunk-hash  spray-mode
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x auth-filter

Applies the specified filter on the interface.

Syntax **dot1x auth-filter** *filter-id vlan-id*

no dot1x auth-filter *filter-id vlan-id*

Command Default There are no filters applied on the interface.

Parameters *filter-id*

Specifies the filter ID to be applied on the interface.

vlan-id

Specifies the VLAN ID.

Modes Interface configuration mode.

Usage Guidelines The **no** form of the command disable the dot1x auth-filter functionality. If the VLAN is not specified, the auth-default-vlan is used.

The following rules apply when using the **dot1x auth-filter** command:

- The maximum number of filters that can be bound to a port is limited by the mac-filter-port default or a configured value.
- The filters must be applied as a group. For example, if you want to apply four filters to an interface, they must all appear on the same command line.
- You cannot add or remove individual filters in the group. To add or remove a filter on an interface, apply the filter group again containing all the filters you want to apply to the port.
- If you apply a filter group to a port that already has a filter group applied, the older filter group is replaced by the new filter group.
- If you add filters to or modify the dot1x authentication filter, the system clears all 802.1X sessions on the port. Consequently, all users that are logged in will need to be re-authenticated.

Examples The following example applies the dot1x filter on a specific VLAN.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# dot1x auth-filter 1 2
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x enable

Enables dot1x authentication.

Syntax **dot1x enable**

dot1x enable all

dot1x enable ethernet *stackid*/*slot*/*port*

no dot1x enable [**all** | **ethernet** *stackid*/*slot*/*port*]

Command Default dot1x authentication is not enabled.

Parameters **all**

Enables dot1x authentication on all interfaces.

ethernet *stackid*/*slot*/*port*

Enables dot1x authentication on the specified interface.

Modes Authentication mode.

Usage Guidelines The **no** form of the command disables dot1x authentication.

Examples The following example enables dot1x authentication on all interfaces.

```
device(config)# authentication
device(config-authen)# dot1x enable all
```

The following example shows enabling dot1x authentication on ethernet interface 1/1/1.

```
device(config)# authentication
device(config-authen)# dot1x enable ethernet 1/1/1
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x guest-vlan

Specifies the guest VLAN ID at the global level.

Syntax **dot1x guest-vlan** *vlan-id*

no dot1x guest-vlan *vlan-id*

Command Default The guest VLAN ID is not specified.

Parameters *vlan-id*

Specifies the VLAN ID of the guest VLAN.

Modes dot1x configuration mode.

Usage Guidelines The **no** form of this command disables the functionality.

Use this command when the client does not support the dot1x authentication, so that the client can access default privileges.

Examples The following example specifies the guest VLAN.

```
device(config)# authentication
device(config-authen)# dot1x guest-vlan 7
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x max-reauth-req

Specifies the maximum number of Extensible Authentication Protocol (EAP) frame retransmissions.

Syntax **dot1x max-reauth-req** *count*

no dot1x max-reauth-req *count*

Command Default The EAP frame retransmissions are not specified.

Parameters *count*

Specifies the EAP frame re-transmissions. This is a number from 1 through 10. The default is 2.

Modes Authentication mode.

Usage Guidelines The **no** form of this command will disable this functionality.

The Brocade device retransmits the EAP-request/identity frame a maximum of two times. If no EAP response/identity frame is received from the client after two EAP-request/identity frame re-transmissions (or the amount of time specified with the max-reauth-req command), the device restarts the authentication process with the client.

You can optionally change the number of times the Brocade device should retransmit the EAP request/identity frame.

Examples The following example configures the device to retransmit an EAP-request/identity frame to a client a maximum of three times.

```
device(config)# authentication
device(config-authen)# dot1x max-reauth-req 3
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x-mka-enable

Enables MACsec Key Agreement (MKA) capabilities on a licensed device and enters dot1x-mka configuration mode.

Syntax

dot1x-mka-enable

no dot1x-mka-enable

Command Default

No MACsec capability is available.

Modes

Global configuration

Usage Guidelines

This command is supported only on the Brocade ICX 6610.

The **no** form of this command disables the MKA and MACsec functionality on all ports. This may require the already authenticated hosts to re-authenticate.

Use the **dot1x-mka-enable** command to enable MACsec on an already licensed device. Commands may be visible, but they do not work on a non-licensed device.

Examples

The following example enables MACsec capabilities on the device.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)#
```

History

Release version	Command history
08.0.20	This command was introduced.

Related Commands

enable-mka, mka-cfg-group

dot1x timeout

Describes the timeout parameters applicable to the device.

Syntax **dot1x timeout** {**quiet-period** *seconds*| **tx-period** *seconds* | **supplicant** *seconds* }

no dot1x timeout {**quiet-period** *seconds*| **tx-period** *seconds* | **supplicant** *seconds* }

Command Default The timeout parameters are not applied to the device.

Parameters **quiet-period** *seconds*

Specifies the time, in seconds, that the device waits before trying to re-authenticate the client. The quiet period can be from 1 through 4294967295 seconds. The default is 60 seconds. If the Brocade device is unable to authenticate the client, the Brocade device waits a specified amount of time before trying again. The amount of time the Brocade device waits is specified with the quiet period parameter.

tx-period *seconds*

Specifies the EAP request retransmission interval, in seconds, with the client. By default, if the Brocade device does not receive an EAP-response/identity frame from a client, the device waits 30 seconds, then retransmits the EAP-request/identity frame. You can optionally change the amount of time the Brocade device waits before re-transmitting the EAP-request/identity frame to the client. If the client does not send back an EAP-response/identity frame within 60 seconds, the device will transmit another EAP-request/identity frame. The tx-period is a value from 1 through 4294967295. The default is 30 seconds.

supplicant *seconds*

By default, when the Brocade device relays an EAP-Request frame from the RADIUS server to the client, it expects to receive a response from the client within 30 seconds. You can optionally specify the wait interval using the **supplicant** *seconds* parameters.

Modes Authentication mode.

Usage Guidelines The **no** form of the command disables dot1x timeout.

Examples The following example specifies the quiet period as 30 seconds.

```
device(config)# authentication
device(config-authen)# dot1x enable
device(config-authen)# dot1x timeout quiet-period 30
```

History

Release version	Command history
08.0.20	This command was introduced.

egress-buffer-profile

Attaches a user-configured egress buffer profile to one or more ports.

Syntax **egress-buffer-profile** *profile-name*

no egress-buffer-profile *profile-name*

Command Default If a port is not attached to a user-configured egress buffer profile, it uses the default egress buffer profile.

Parameters *profile-name*

Specifies the name of the egress buffer profile to be attached to the port.

Modes Interface mode

Multiple-interface mode

Usage Guidelines The **no** form of this command removes a user-configured egress buffer profile from the port and the port uses the default egress buffer profile.

You must configure an egress buffer profile before you can attach it to a port.

Only one egress buffer profile at a time can be attached to any port. You can attach an egress buffer profile to more than one port.

Examples The following example attaches an egress buffer profile named egress1 to a port:

```
Device(config-if-e10000-1/1/1)# egress-buffer-profile egress1
```

The following example attaches an egress buffer profile named egress2 to multiple ports:

```
Device(config-mif-1/1/2-1/1/16)# egress-buffer-profile egress2
```

The following example removes an egress buffer profile named egress2 from multiple ports:

```
Device(config-mif-1/1/2-1/1/16)# no egress-buffer-profile egress2
```

History

Release version	Command history
8.0.10	This command was introduced.

enable-accounting

Enables Access Control List (ACL) accounting for IPv4 and IPv6 named ACLs.

Syntax **enable-accounting**

no enable-accounting

Command Default This option is disabled.

Modes IPv4 and IPv6 access-list configuration modes

Usage Guidelines This is only applicable to named ACLs. The **no** form of this command disables ACL accounting on the associated ACL interface.

Examples The following example enables IPv6 ACL accounting. The named access-list must be configured before enabling the ACL accounting.

```
device(config)# ipv6 access-list v6
device(config-ipv6-access-list-v6)# enable-accounting
```

The following example enables ACL accounting for an IPv4 named ACL.

```
device(config)# ip access-list standard std
device(config-std-nacl)# permit 10.10.10.0/24
device(config-std-nacl)# deny 10.20.20.0/24
device(config-std-nacl)# enable-accounting
```

History

Release version	Command history
08.0.10	This command was introduced.

enable-mka

Enables MACsec Key Agreement (MKA) on a specified interface and changes the mode to dot1x-mka-interface mode to enable related parameters to be configured.

Syntax **enable-mka ethernet** *device/slot/port*

no enable-mka ethernet *device/slot/port*

Command Default MKA is not enabled on an interface.

Parameters **ethernet** *device/slot/port*

Specifies an Ethernet interface and the number of the device, the slot on the device, and the port on that slot.

Modes dot1x-mka-interface mode

Usage Guidelines When the **no** version of the command is executed, MACSec is removed from the port.

This command is supported only on the Brocade ICX 6610.

For a MACsec channel to be created between two ports, both ports and devices designated must have MACsec enabled and configured.

Examples The following example enables MACsec on port 2, slot 3 of the first device in the stack.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/3/2
device(config-dot1x-mka-1/3/2)#
```

History

Release version	Command history
08.0.20	This command was introduced.

errdisable packet-inerror-detect

Enables the device to monitor configured ports for inError packets and defines the sampling time interval in which the number of inError packets is counted.

Syntax **errdisable packet-inerror-detect** *sampling-interval*

no errdisable packet-inerror-detect *sampling-interval*

Command Default There is no monitoring for inError packets on any port of the device.

Parameters *sampling-interval*

Specifies the sampling interval in seconds. It can take a value in the inclusive range of 2 through 60 seconds.

Modes Global configuration mode

Usage Guidelines If the number of inError packets exceeds the configured threshold for two consecutive sampling windows, then the configured port is error-disabled. The **no** form of this command disables this monitoring.

Examples The following example sets the sampling interval in which the number of inError packets is counted to three seconds.

```
device(config)# errdisable packet-inerror-detect 3
```

History

Release version	Command history
07.3.00g	This command was introduced.

Commands K - S

key-server-priority

Configures the MACsec key-server priority for the MACsec Key Agreement (MKA) group.

Syntax **key-server-priority** *value*

no key-server-priority *value*

Command Default Key-server priority is set to 16. This is not displayed in configuration details.

Parameters *value*

Specifies key-server priority. The possible values range from 0 to 255, where 0 is highest priority and 255 is lowest priority.

Modes dot1x-mka-cfg-group mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

The **no** form of the command removes the previous priority setting.

During key-server election, the server with the highest priority (the server with the lowest key-server priority value) becomes the key-server.

Examples The following example sets the key-server priority for MKA group test1 to 5.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# key-server-priority 5
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was modified. The key-server priority value range was increased from 0 through 127 to 0 through 255.

link-config gig copper autoneg-control

Configures the maximum advertised speed on a port that has auto-negotiation enabled.

Syntax **link-config gig copper autoneg-control** { **100m-auto** | **10m-auto** | **down-shift** } **ethernet** *stack-id/slot/port* [**to** *stack-id/slot/port* | [**ethernet** *stack-id/slot/port* **to** *stack-id/slot/port* | **ethernet** *stack-id/slot/port*] ...]

no link-config gig copper autoneg-control { **100m-auto** | **10m-auto** | **down-shift** } **ethernet** *stack-id/slot/port* [**to** *stack-id/slot/port* | [**ethernet** *stack-id/slot/port* **to** *stack-id/slot/port* | **ethernet** *stack-id/slot/port*] ...]

Command Default The maximum port speed advertisement is not configured.

Parameters **ethernet** *stack-id/slot/port*

Specifies the Ethernet interface.

Modes Global configuration mode

Usage Guidelines Maximum port speed advertisement is not supported on Brocade ICX 7750.

The **down-shift** option is not supported on Brocade ICX 7450.

The maximum port speed advertisement works only when auto-negotiation is enabled (CLI command **speed-duplex auto**). If auto-negotiation is off, the device rejects the maximum port speed advertisement configuration.

You can enable the maximum port speed advertisement on one or two ports at a time.

When **port speed down-shift** or the maximum port speed advertisement is enabled on a port, the device rejects any configuration attempts to set the port to a forced speed mode (100 Mbps or 1000 Mbps).

The **no** form of the command disables the maximum port speed advertisement.

Examples The following command configures a maximum port speed advertisement of 10 Mbps on a port that has auto-negotiation enabled.

```
device(config)# link-config gig copper autoneg-control 10m-auto ethernet 1/1/1
```

History

Release version	Command history
8.0.20	This command was introduced in Brocade ICX 7450, but the **downshift** option was not supported.

logging

Enables logging on the Router Advertisement (RA) guard policy.

Syntax **logging**

no logging

Modes RA guard policy configuration mode

Usage Guidelines The **no** form of this command disables logging on the policy.

Logging cannot be modified if the RA guard policy is in use.

You can verify the logs for RA guard, such as RAs dropped, permitted, count for dropped packets, and reasons for the drop.

Logging increases the CPU load and for higher traffic rates, RA packets drop due to congestion if they are received at the line rate. For less load on the CPU, logging can be disabled on the RA guard policy.

Examples The following example enables logging on an RA guard policy:

```
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# logging
```

logging cli-command

Enables logging of all syntactically valid CLI commands from each user session into the system log.

Syntax **logging cli-command**

no logging cli-command

Command Default Logging of CLI commands is not enabled.

Modes Global configuration mode

Usage Guidelines If the **logging cli-command** command is configured, all the CLI commands executed by the user are logged in the system log and are displayed in the **show logging** command output.

The **no** form of the command disables the logging of CLI commands from each user session into the system log.

Examples The following example enables the logging of CLI commands on the device.

```
device(config)# logging cli-command
```

The following example shows the system log records which are displayed in the **show logging** command output. The system log contains the valid commands that are executed by the user.

```
Brocade (config)#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 5 overruns)
            Buffer logging: level ACDMEINW, 50 messages logged
            level code: A=alert C=critical D=debugging M=emergency E=error
I=informational N=notification W=warning
Dynamic Log Buffer (50 lines):
8d02h28m43s:I:CLI CMD: "ip route 0.0.0.0 0.0.0.0 10.20.64.1" by un-authenticated
user from console
8d02h28m24s:I:System: Interface ethernet 1/1, state up
8d02h28m22s:I:CLI CMD: "enable" by un-authenticated user from console
8d02h28m22s:I:PORT: 1/1 enabled by un-authenticated user from console session
8d02h28m19s:I:CLI CMD: "disable" by un-authenticated user from console
8d02h28m19s:I:PORT: 1/1 disabled by un-authenticated user from console session
8d02h28m16s:I:CLI CMD: "interface ethernet 1/1" by un-authenticated user from
console
```

loop-detection shutdown-disable

Disables shutdown of a port when a loop detection probe packet is received on an interface.

Syntax **loop-detection shutdown-disable**

no loop-detection shutdown-disable

Command Default Loop detection shutdown is enabled on the interface.

Modes Interface configuration

Usage Guidelines The **no** form of this command disables loop detection shutdown.

Shutdown prevention for loop-detect functionality allows users to disable shut down of a port when the loop detection probe packet is received on an interface. This provides control over deciding which port is allowed to enter in to an error-disabled state and go into a shutdown state when a loop is detected.

Examples The following example disables loop detection shutdown on an interface.

```
device(config)# interface ethernet 1/7
device(config-if-e1000-1/7)# loop-detection shutdown-disable
```

History

Release version	Command history
08.0.20	This command was introduced.

loop-detection-syslog-interval

Specifies the interval (in minutes) at which a syslog is generated.

Syntax **loop-detection-syslog-interval** *num*

no loop-detection-syslog-interval *num*

Command Default The syslog interval is 5 minutes.

Parameters *num*

Specifies the syslog interval in minutes. The interval can range from 1 through 1440 minutes.

Modes Global configuration

Usage Guidelines The **no** form of this command restores the default settings.

You can specify the interval at which the loop detection syslog message is generated if the **loop-detection-shutdown-disable** command is configured for the port. This configuration applies to all the ports that have loop detection shutdown prevention configured.

Examples The following example shows the loop detection syslog interval set to 1 hour.

```
device(config)# loop-detection-syslog-interval 60
```

History

Release version	Command history
08.0.20	This command was introduced.

mac filter enable-accounting

Enables access control list (ACL) accounting on Layer 2 MAC filters.

Syntax **mac filter** *num* **enable-accounting**

no mac filter *num* **enable-accounting**

Command Default This option is disabled.

Parameters *num*

Specifies the MAC filter ID.

enable-accounting

Enables MAC filter accounting on the specified interface.

Modes Global configuration mode

Usage Guidelines The **no** form of this command disables ACL accounting on the associated Layer 2 MAC filter interface.

Examples The following example enables ACL accounting on a Layer 2 MAC filter.

```
device(config)# mac filter 1 permit 0000.0000.0001 ffff.ffff.ffff any
device(config)# mac filter 1 enable-accounting
device(config)# interface ethernet 3/21
device(config-if-e1000-3/21)# mac filter-group 1
```

History

Release version	Command history
08.0.10	This command was introduced.

mac-auth auth-filter

Applies the specified filter on the interface.

Syntax **mac-auth auth-filter** *filter-id* **vlan** *vlan-id*

no mac-auth auth-filter *filter-id* **vlan** *vlan-id*

Command Default There are no filters applied on the interface.

Parameters *filter-id*

Specifies the identification number of the filter to be applied on the interface.

vlan *vlan-id*

Specifies the identification number of the VLAN to which the filter is applied.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command disables this functionality.

You must use the interface configuration mode to use this command.

If the VLAN is not specified in the command, the auth-default VLAN is used.

Examples The following example applies the MAC address filter on VLAN 2.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mac-auth auth-filter 1 vlan 2
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-auth dot1x-override

Configures the device to perform dot1x authentication when MAC authentication fails.

Syntax **mac-auth dot1x-override**

no mac-auth dot1x-override

Command Default MAC authentication dot1x override is not enabled.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables MAC authentication dot1x override functionality.

Examples The following example enables MAC authentication dot1x override when MAC authentication fails.

```
device(config)# authentication
device(config-authen)# mac-auth dot1x-override
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-auth enable

Enables MAC authentication globally or on a specific interface.

Syntax **mac-auth enable** [**all** | **ethernet** *device*/*slot*/*port*]

no mac-auth enable [**all** | **ethernet** *device*/*slot*/*port*]

Command Default MAC authentication is not enabled.

Parameters **all**

Enables MAC authentication on all interfaces.

ethernet *device*/*slot*/*port*

Enables MAC authentication on a specific interface.

Modes Authentication mode.

Usage Guidelines The **no** form of the command disables MAC authentication.

Examples The following example globally enables MAC authentication.

```
device(config)#authentication
device(config-authen)#mac-auth enable
device(config-authen)#mac-auth enable all
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-auth password-format

Configures the MAC authentication password format.

Syntax **mac-auth password-format** { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** } [upper-case]

no mac-auth password-format { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** } [upper-case]

Command Default By default, the MAC address is sent to the RADIUS server in the format xxxxxxxxxxxx in lower case.

Parameters

xx-xx-xx-xx-xx-xx

Specifies the MAC authentication password format as xx-xx-xx-xx-xx-xx.

xxxx.xxxx.xxxx

Specifies the MAC authentication password format as xxxx.xxxx.xxxx.

xxxxxxxxxxxx

Specifies the MAC authentication password format as xxxxxxxxxxxx.

upper-case

Converts the password to uppercase.

Modes Authentication mode

Usage Guidelines The **no** form of the command restores the default (no MAC authentication password format is configured).

You can configure the device to send the MAC address to the RADIUS server in the format xx-xx-xx-xx-xx-xx, or the format xxxx.xxxx.xxxx. Use the **upper-case** password format option to send the password in uppercase.

Examples The following example configures the MAC authentication password format as xx-xx-xx-xx-xx-xx.

```
device(config)# authentication
device(config-authen)# mac-auth password-format xx-xx-xx-xx-xx-xx
```

The following example configures the MAC authentication password format as xx-xx-xx-xx-xx-xx in upper case.

```
device(config)# authentication
device(config-authen)# mac-auth password-format xx-xx-xx-xx-xx-xx upper-case
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20c	The **upper-case** option was added.

mac-auth password-override

Enables password override for MAC authentication. The password you specify is used for MAC authentication instead of the MAC address.

Syntax **mac-auth password-override** *password*

no mac-auth password-override *password*

Command Default MAC authentication password override is not enabled.

Parameters *password*

Specifies the password to be used for MAC authentication. The password can contain up to 32 alphanumeric characters, but cannot include blank spaces.

Modes Authentication mode

Usage Guidelines The **no** form disables MAC authentication password override.

The MAC address is still the user name and cannot be changed.

Examples The following example enables MAC authentication password override on the device.

```
device(config)# authentication
device(config-authen)# mac-auth password-override password
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-notification interval

Configures the MAC-notification interval between each set of generated traps.

Syntax **mac-notification interval** *secs*

no mac-notification interval *secs*

Command Default No interval for MAC-notification is configured.

Parameters *secs*

Specifies the MAC-notification interval in seconds between each set of traps that are generated. The range is from 1 through 3600 seconds (1 hour). The default interval is 3 seconds.

Modes Global configuration mode

Usage Guidelines The **no** form of this command sets the interval to its default value, which is 3 seconds.

A trap is sent aggregating the MAC events such as addition or deletion depending on the interval you specify.

Examples The following example configures an interval of 40 seconds.

```
device(config)# mac-notification interval 40
```

The following example sets the interval to its default value:

```
device(config)# no mac-notification interval 3
```

History

Release version	Command history
08.0.10	This command was introduced.

macsec cipher-suite

Enables GCM-AES-128 bit encryption or GCM-AES-128 bit integrity checks on MACsec frames transmitted between group members.

Syntax **macsec cipher-suite** { **gcm-aes-128** | **gcm-aes-128 integrity-only** }

no macsec cipher-suite { **gcm-aes-128** | **gcm-aes-128 integrity-only** }

Command Default GCM-AES-128 bit encryption or integrity checking is not enabled. Frames are encrypted starting with the first byte of the data packet, and ICV checking is enabled.

Parameters

gcm-aes-128

Enables GCM-AES-128 bit encryption.

gcm-aes-128 integrity-only

Enables GCM-AES-128 bit integrity checks.

Modes dot1x-mka-cfg-group mode

Usage Guidelines The **no** form of the command restores the default encryption and integrity checking.

This command is supported only on the Brocade ICX 6610.

The **macsec cipher-suite** command can be used in conjunction with an encryption offset configured with the **macsec confidentiality-offset** command.

Examples The following example enables GCM-AES-128 encryption on group test1.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
```

The following example enables GCM-AES-128 bit integrity checking on test1.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128 integrity-only
```

History

Release version	Command history
08.0.20	This command was introduced.

macsec confidentiality-offset

Configures the offset size for MACsec encryption.

Syntax **macsec confidentiality-offset** *size*

no macsec confidentiality-offset *size*

Command Default No offset for MACsec encryption is configured.

Parameters *size*

Determines where encryption begins. Valid values are:

30	Encryption begins at byte 31 of the data packet.
50	Encryption begins at byte 51 of the data packet.

Modes dot1x-mka-cfg-group mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

The **no** form of the command disables encryption offset on all interfaces in the MACsec MKA group.

This command is only meaningful when encryption is enabled for the MACsec group using the **macsec cipher-suite** command.

Examples The following example configures a 30-byte offset on encrypted transmissions as part of group test1 parameters.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
```

History

Release version	Command history
08.0.20	This command was introduced.

macsec frame-validation

Enables validation checks for frames with MACsec headers and configures the validation mode (strict or not strict).

Syntax **macsec frame-validation** { **disable** | **check** | **strict** }

no macsec frame-validation { **disable** | **check** | **strict** }

Command Default MACsec frame validation is disabled (not visible in configuration).

Parameters

disable

Disables validation checks for frames with MACsec headers.

check

Enables validation checks for frames with MACsec headers and configures non-strict validation mode. If frame validation fails, counters are incremented but packets are accepted.

strict

Enables validation checks for frames with MACsec headers and configures strict validation mode. If frame validation fails, counters are incremented and packets are dropped.

Modes dot1x-mka-cfg-group mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

The **no** form of the restores the default (validation checks for frames with MACsec headers is disabled).

Examples The following example enables validation checks for frames with MACsec headers on group test1 and configures strict validation mode.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec frame-validation strict
```

History

Release version	Command history
08.0.20	This command was introduced.

macsec replay-protection

Specifies the action to be taken when packets are received out of order, based on their packet number. If replay protection is configured, you can specify the window size within which out-of-order packets are allowed.

Syntax **macsec replay-protection** { **strict** | **out-of-order window-size** *size* }

no macsec replay-protection { **strict** | **out-of-order window-size** *size* }

Parameters

strict

Does not allow out-of-order packets.

out-of-order window-size

Allows out-of-order packets within a specific window size.

size

Specifies the allowable window within which an out-of-order packet can be received. Allowable range is from 0 through 4294967295.

Modes dot1x-mka-cfg-group mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

The **no** form of the command disables macsec replay protection.

Examples The following example configures group test1 to accept packets in exact sequence only.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec replay-protection strict
device(config-dot1x-mka-group-test1)#
```

The following example configures group test1 to accept out-of-order MACsec frames within a window size of 2000.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec replay-protection out-of-order window-
size 2000
```

History

Release version	Command history
08.0.20	This command was introduced.

max-hw-age

Enables and configures the maximum hardware age for denied MAC addresses.

Syntax **max-hw-age** *age*

no max-hw-age *age*

Command Default The maximum hardware age is not configured. The default hardware aging time is 70 seconds.

Parameters *age*

Specifies the maximum hardware age in seconds. The possible values range from 1 to 65535 seconds.

Modes Authentication mode

Usage Guidelines The **no** form of this command disables maximum hardware age.

Aging of the Layer 2 hardware entry for a blocked MAC address occurs in two phases, known as hardware aging and software aging. On FastIron devices, the hardware aging period for blocked MAC addresses is fixed at 70 seconds and is non-configurable. The hardware aging time for non-blocked MAC addresses is the length of time specified with the **mac-age** command. The software aging period for blocked MAC addresses is configurable through the CLI. Once the hardware aging period ends, the software aging period begins. When the software aging period ends, the blocked MAC address ages out, and can be authenticated again if the Brocade device receives traffic from the MAC address.

On FastIron X Series devices, the hardware aging period for blocked MAC addresses is not fixed at 70 seconds. The hardware aging period for blocked MAC addresses is equal to the length of time specified with the **mac-age** command. As on FastIron devices, once the hardware aging period ends, the software aging period begins. When the software aging period ends, the blocked MAC address ages out, and can be authenticated again if the device receives traffic from the MAC address.

Examples The following example enables maximum hardware age and sets it to 160 seconds.

```
device(config)# authentication
device(config-authen)# max-hw-age 160
```

History

Release version	Command history
08.0.20	This command was introduced.

maximum-preference

Configures the Router Advertisement (RA) guard policy to accept RAs based on a router preference setting.

Syntax **maximum-preference** { **high** | **low** | **medium** }

no maximum-preference { **high** | **low** | **medium** }

Command Default

The router preference setting for the RA guard policy is high (allows all RAs).

Parameters

high

Configures the router preference of RAs for the RA guard policy to high (allows all RAs). This is the default.

low

Allows RAs of low router preference.

medium

Allows RAs of low and medium router preference.

Modes RA guard policy configuration mode

Usage Guidelines If a very low value is set, the RAs expected to be forwarded might get dropped.

The **no** form of this command removes the router preference for an RA guard policy.

Examples The following example configures the RA guard policy router preference to low:

```
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# maximum-preference low
```

max-mcache

Configures the maximum number of PIM cache entries.

Syntax **max-mcache** *num*

no max-mcache *num*

Command Default If this command is not configured, the maximum value is determined by the **system max pim-hw-mcache** command or by available system resources.

Parameters *num*

Specifies the maximum number of multicast cache entries for PIM.

Modes PIM router configuration mode

PIM router VRF mode

Usage Guidelines The **no** form of this command removes the configuration and resets the command to its default behavior.

Configure the **max-mcache** command to define the maximum number of repeated cache entries for PIM traffic being sent from the same source address and being received by the same destination address. To define this maximum for the default VRF, configure the command in router PIM configuration mode; to define the maximum for a specific VRF, first configure the **router pim vrf** command.

Examples This example configures the maximum number of PIM cache entries for the default VRF to 999.

```
device(config)# router pim
device(config-pim-router)# max-mcache 999
```

This example configures the maximum number of PIM cache entries for the VRF, VPN1, to 999.

```
device(config)# router pim vrf vpn1
device(config-pim-router-vrf-vpn1)# max-mcache 999
```

max-sw-age

Configures the maximum software age for denied MAC addresses.

Syntax **max-sw-age** *age*

no max-sw *age*

Command Default The maximum software age is not configured.

Parameters *age*

You can specify from 1 - 65535 seconds. The default is 120 seconds.

Modes Authentication mode

Usage Guidelines When the Brocade device is configured to drop traffic from non-authenticated MAC addresses, traffic from the blocked MAC addresses is dropped in hardware, without being sent to the CPU. A Layer 2 CAM entry is created that drops traffic from the blocked MAC address in hardware. If no traffic is received from the blocked MAC address for a certain amount of time, this Layer 2 CAM entry is aged out. If traffic is subsequently received from the MAC address, then an attempt can be made to authenticate the MAC address again.

Aging of the Layer 2 CAM entry for a blocked MAC address occurs in two phases, known as hardware aging and software aging. The hardware aging period is fixed at 70 seconds and is non-configurable. The software aging time is configurable through the CLI.

Examples The following example configures the maximum software age to 170 seconds.

```
device(config)# authentication
device(config-authen)# max-sw-age 170
```

History

Release version	Command history
08.0.20	This command was introduced.

mesh-group

Configures a multicast source discovery protocol (MSDP) mesh group from several rendezvous points (RPs).

Syntax **mesh-group** *group-name peer-address*

no mesh-group *group-name peer-address*

Command Default Mesh groups are not configured.

Parameters *group-name*

Specifies the mesh group as alphabetic characters. The limit is 31 characters.

peer-address

Specifies the IP address of the MSDP peer that is being placed in the mesh group. Each mesh group can include up to 32 peers.

Modes MSDP VRF configuration mode

Usage Guidelines The **no** form of this command removes mesh groups.

You must configure the **msdp-peer** command to configure the MSDP peers by assigning their IP addresses and the loopback interfaces before you configure a mesh group.

You can have up to four mesh groups in a multicast network. Each mesh group can include up to 15 peers.

Each device that will be part of a mesh group must have a mesh group definition for all the peers in the mesh-group.

Examples This example configures an MSDP mesh group on each device that will be included in the mesh group.

```
Device(config)# router msdp
Device(config-msdp-router)# msdp-peer 206.251.18.31 connect-source loopback 2
Device(config-msdp-router)# msdp-peer 206.251.19.31 connect-source loopback 2
Device(config-msdp-router)# msdp-peer 206.251.20.31 connect-source loopback 2
Device(config-msdp-router)# mesh-group GroupA 206.251.18.31
Device(config-msdp-router)# mesh-group GroupA 206.251.19.31
Device(config-msdp-router)# mesh-group GroupA 206.251.20.31
Device(config-msdp-router)# exit
```

message-interval

Changes the default PIM Sparse join or prune message interval.

Syntax **message-interval** [**vrf** *vrf-name*] *interval*

no message-interval [**vrf** *vrf-name*] *interval*

Parameters **vrf** *vrf-name*

Specifies a VRF instance.

interval

Specifies the join or prune message interval in seconds. The range is 10 through 18724; the default is 60.

Command Default The join or prune interval is 60 seconds.

Modes PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines The **no** form of this command restores the default; the join-prune interval is 60 seconds.

PIM Sparse join and prune messages inform other PIM Sparse routers about clients who want to become receivers (join) or stop being receivers (prune) for PIM Sparse groups.

NOTE
Configure the same join or prune message interval on all the PIM Sparse routers in the PIM Sparse domain. The performance of PIM Sparse can be adversely affected if the routers use different timer intervals.

Examples This example changes the PIM join or prune interval to 30 seconds.

```
Device(config)# ipv6 router pim
Device(config-ipv6-pim-router)# message-interval 30
```

This example changes the PIM join or prune interval on a VRF to 30 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# message-interval 30
```

mka-cfg-group

Creates and names a MACsec Key Agreement (MKA) configuration group.

Syntax **mka-cfg-group** *group-name*

no mka-cfg-group *group-name*

Command Default No MACsec options are configured for an MKA configuration group. All related parameters retain their default settings.

Parameters *group-name*

Provides a name for an MKA configuration group that can be applied to ports.

Modes dot1x-mka configuration mode

dot1x-mka-interface configuration mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

The **no** form of this command deletes the MKA configuration group. MACSec is disabled on the ports where the group is configured.

The **dot1x-mka-enable** command must be executed before the **mka-cfg-group** command can be used.

After the MACsec Key Agreement (MKA) configuration group is created, you can apply the configured group and its settings to an interface being configured using the **mka-cfg-group** command in the dot1x-mka-interface configuration mode.

Examples The following example creates the MKA configuration group test1.

```
device(config)# dot1x-mka
  dot1x-mka-enable              Enable MACsec
device(config)# dot1x-mka-enable
device(config-dot1x-mka)#
device(config-dot1x-mka)# mka-cfg-group
  ASCII string   Name for this group
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# key-server-priority
  DECIMAL   Priority of the Key Server. Valid values should be between 0 and 255
device(config-dot1x-mka-group-test1)# key-server-priority 5
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec cipher-suite
  gcm-aes-128   GCM-AES-128 Cipher suite
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec confidentiality-offset
  30   Confidentiality offset of 30
  50   Confidentiality offset of 50
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec frame-validation
  check     Validate frames with secTAG and accept frames without secTAG
  disable   Disable frame validation
  strict    Validate frames with secTAG and discard frames without secTAG
device(config-dot1x-mka-group-test1)# macsec frame-validation strict
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec replay-protection
  out-of-order   Validate MACsec frames arrive in the given window size
  strict         Validate MACsec frames arrive in a sequence
device(config-dot1x-mka-group-test1)# macsec replay-protection strict
device(config-dot1x-mka-group-test1)#
```

The following example applies the previously configured MKA group test1 to ethernet interface 1/3/3.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/3/3
device(config-dot1x-mka-1/3/3)# mka-cfg-group test1
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was expanded to support the association of a configured MKA group and its settings to an interface at the interface configuration level. The **mka-group** command was deprecated as part of this change.

mstp instance

Configures a Multiple Spanning Tee Protocol (MSTP) instance that allows multiple VLANs to be managed by a single STP instance and supports per-VLAN STP. This allows you to use fewer spanning-tree instances to map to VLANs.

Syntax **mstp instance** *instance-number* [**vlan** *vlan-id* | **vlan-group** *group-id*] [**priority** *priority-value*]

no mstp instance *instance-number* [**vlan** *vlan-id* | **vlan-group** *group-id*] [**priority** *priority-value*]

Command Default No MSTP instances are configured. Any VLANs remain in the common, internal spanning tree (CIST) or are free.

Parameters *instance-number*

Specifies the number for the instance of MSTP that you are configuring. You can specify up to 15 instances, identifying each, in MSTP mode, by a number in the range 1 through 4094. In MSTP mode, you cannot specify the value 0, which identifies the CIST. In MSTP+ mode, the range is 0 through 4094.

vlan *vlan-id*

Assigns one or more VLANs or a range of VLANs to the MSTP instance.

vlan-group *group-id*

Assigns one or more VLAN groups to the MSTP instance.

priority *priority-value*

Specifies the forwarding preference for instances within a VLAN or on the device. You can specify a numeric value in the range 0 to 61440 in increments of 4096. A higher priority variable means a lower forwarding priority. The default value is 32768.

Modes Global configuration mode

Usage Guidelines In MSTP mode, the **no** form of this command moves a VLAN or VLAN group from its assigned MSTP back into the CIST. In MSTP+ mode, the **no** form of this command assigns any VLAN as a free VLAN.

The system does not allow an MSTP instance without any VLANs mapped to it;removing all VLANs from an MSTP instance deletes the instance from the system.

In MSTP+ mode, you can specify an instance number value of 0 because MSTP+ mode allows you to add VLANs to and remove VLANs from the CIST.

Examples The following example configures an MSTP instance and map VLANs 1 to 7 to it.

```
Device(config)# mstp instance 7 vlan 4 to 7
```

The following example specifies a priority of 8192 to MSTP instance 1.

```
Device(config)# mstp instance 1 priority 8192
```

mstp scope

Configures VLANs in Multiple Spanning Tee Protocol (MSTP) mode.

Syntax **mstp scope** { **all** | **pvst** }

no mstp scope { **all** | **pvst** }

Command Default No VLAN is under direct MSTP control.

Parameters **all**

Configures MSTP on all VLANs.

pvst

Configures MSTP in per-VLAN spanning tree (PVST) mode.

Modes Global configuration mode

Usage Guidelines The **no** form of this command removes the MSTP PVST mode and restores the device to non-MSTP mode.

MSTP is not operational until the **mstp start** command is configured. You cannot start MSTP+ unless at least one MSTP+ instance of MSTP+ is configured.

Examples The following example configures MSTP mode on all VLANs.

```
Device(config)# mstp scope all
```

The following example enables MSTP in PVST mode.

```
Device(config)# mstp scope pvst
```

History

Release version	Command history
8.0.20	This command was modified to support the **pvst** keyword.

multicast disable-pimsm-snoop

Disables PIM Sparse mode (SM) snooping for a specific VLAN when snooping is enabled globally.

Syntax **multicast disable-pimsm-snoop**

no multicast disable-pimsm-snoop

Command Default The global PIM SM snooping setting applies.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the global PIM SM snooping setting.

Examples This example disables PIM SM snooping on VLAN 20.

```
Device(config)#config vlan 20
Device(config-vlan-20)#multicast disable-pimsm-snoop
```

multicast fast-convergence

Configures a device to listen to topology change events in Layer 2 protocols such as spanning tree, and then send general queries to shorten the convergence time.

Syntax **multicast fast-convergence**

no multicast fast-convergence

Command Default Fast convergence is not configured.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default; fast convergence is not configured.

If the Layer 2 protocol cannot detect a topology change, fast convergence may not work in some cases. For example, if the direct connection between two devices switches from one interface to another, the Rapid Spanning Tree protocol (802.1w) considers this optimization rather than a topology change. In this example, other devices do not receive topology change notifications, and cannot send queries to speed up the convergence. Fast convergence works well with the regular spanning tree protocol in this case.

Examples This example configures fast convergence on VLAN 70.

```
Device(config)#vlan 70
Device(config-vlan-70)#multicast fast-convergence
```

multicast fast-leave-v2

Configures fast leave for IGMP V2.

Syntax **multicast fast-leave-v2**

no multicast fast-leave-v2

Command Default Fast leave for IGMP V2 is not configured.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default; fast leave for IGMP V2 is not configured.

When a device receives an IGMP V2 leave message, it sends out multiple group-specific queries. If no other client replies within the waiting period, the device stops forwarding traffic. When the **multicast fast-leave-v2** command is configured, and when the device receives a leave message, it immediately stops forwarding to that port. The device does not send group specific-queries. When the **multicast fast-leave-v2** command is configured on a VLAN, you must not have multiple clients on any port that is part of the VLAN.

In a scenario where two devices connect, the querier device should not be configured for fast-leave-v2 because the port might have multiple clients through the non-querier.

You can configure the **ip multicast leave-wait-time** command to set the number of queries and the waiting period.

Examples This example configures fast leave for IGMP on VLAN 10.

```
Device(config)#vlan 10
Device(config-vlan-10)#multicast fast-leave-v2
```

multicast pimsm-snooping prune-wait

Configures the amount of time a device waits after receiving a PIM prune message before removing the outgoing interface (OIF) from the forwarding entry.

Syntax **multicast pimsm-snooping prune-wait** *seconds*

no multicast pimsm-snooping prune-wait *seconds*

Command Default The prune-wait time is 5 seconds.

Parameters *seconds*

The time to wait, in seconds. The range is 0 to 65535; the default is 5.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default prune-wait time (5 seconds).

The prune-wait time is necessary on a LAN where multiple receivers could be listening to the group; it gives them time to override the prune message. Configure the **multicast pimsm-snooping prune-wait** command to modify the prune-wait time according to topology and PIM router configurations.

In accordance with RFC 4601, PIM routers delay pruning for 3.5 seconds by default, so configuring a lower prune-wait value may cause traffic disruption. You should configure a prune-wait value lower than 3.5 seconds only if the topology supports it, for example, if the group has only one receiver, and an immediate prune is needed.

Examples The following example configures the prune-wait time to 7 seconds.

```
Device(config)#vlan 10
Device(config-vlan-10)#multicast pimsm-snooping prune-wait 7
```

History

Release version	Command history
8.0.20	This command was introduced.

multicast port-version

Configures the IGMP version on individual ports in a VLAN.

Syntax **multicast port-version** { **2** | **3** } **ethernet** *port* [**ethernet** *port* | **to** *port*]

no multicast port-version { **2** | **3** } **ethernet** *port* [**ethernet** *port* | **to** *port*]

Command Default The port uses the IGMP version configured globally or for the VLAN.

Parameters

2
Configures IGMP version 2.

3
Configures IGMP version 3.

ethernet *port*
Specifies the port to configure the version on.

to
Specifies a range of ports.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the IGMP version configured globally or for the VLAN.

You can specify a list of ports, separated by a space, or a range of ports, or you can combine lists and ranges.

See the description of the **ip multicast version** command for information on how to configure the IGMP version globally.

See the description of the **multicast version** command for information on how to configure the IGMP version on a VLAN.

Examples This example configures ports 4, 5, and 6 to use IGMP version 3.

```
Device(config)#config vlan 20
(config-vlan-20)#multicast port-version 3 ethernet 2/4 to 2/6
```

multicast proxy-off

Turns off proxy activity for static groups.

Syntax **multicast proxy-off**

no multicast proxy-off

Command Default Proxy activity is on.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default; proxy activity is on.

When a device is configured for static groups, it acts as a proxy and sends membership reports for the static groups when it receives general or group-specific queries. When a static group configuration is removed, the group is deleted from the active group table immediately. However, leave messages are not sent to the querier, and the querier must age out the group. You can configure the **multicast proxy-off** command to turn off proxy activity.

Examples This example turns off proxy activity for VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast proxy-off
```

multicast router-port

Configures a static router Ethernet port to receive multicast control and data packets.

Syntax **multicast router-port ethernet** *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

multicast router-port ethernet *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

Command Default The device forwards all multicast control and data packets only to router ports that receive queries.

Parameters *stackid/slot/portnum*

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can configure a single port or a list of ports, separated by a space.

to

Specifies a range of ports.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default, that is, the device forwards all multicast control and data packets only to router ports that receive queries.

Examples This example configures a static port on Ethernet 1/1/3 on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/3
```

This example configures a list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/24 ethernet 1/6/24 ethernet
1/8/17
```

This example configures a range of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/1 to 1/1/8
```

This example configures a combined range and list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/1 to 1/1/8 ethernet 1/1/24
ethernet 1/6/24 ethernet 1/8/17
```

multicast static-group

Configures a static IGMP group for a VLAN.

Syntax **multicast static-group** *ipv4-address* [**count** *num*] [**ethernet** *stackid*|*slot*|*portnum* | **drop**]

no multicast static-group *ipv4-address* [**count** *num*] [**ethernet** *stackid*|*slot*|*portnum* | **drop**]

Command Default The VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports.

Parameters *ipv4-address*

Specifies the address of the static group.

count *num*

Specifies a contiguous range of groups.

ethernet *stackid*|*slot*|*portnum*

Specifies the ports to be included in the group. On standalone devices specify the interface ID in the format slot/port-iD; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID.

drop

Specifies discarding data traffic to a group in hardware.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command removes the static group fromr the VLAN.

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. You can configure the **multicast static-group** command to create a static group that applies to specific ports, allowing packets to be forwarded to them even though they have no client membership reports.

On FCX, ICX 6610, ICX 6430, ICX 6450, and ICX 6650 devices, configuring the **drop** keyword discards data traffic to a group in hardware. The group can be any multicast group including groups in the reserved range of 224.0.0.X. Configuring the **drop** keyword does not affect IGMP packets, which are always trapped to CPU when snooping is enabled. It applies to the entire VLAN, and cannot be configured for a port list. When the **drop** keyword is not configured, the group must exist outside the reserved range.

Examples This example configures on VLAN 20 a static group containing ports 1/1/3 and 1/1/5 to 1/1/7.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast static-group 224.1.1.1 count 2 ethernet 1/1/3
ethernet 1/1/5 to 1/1/7
```

multicast tracking

Enables tracking and fast leave on VLANs.

Syntax **multicast tracking**

no multicast tracking

Command Default Tracking and fast leave are disabled.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default, that is, tracking and fast leave are disabled.

The membership tracking and fast leave features are supported for IGMP V3 only. If any port or any client is not configured for IGMP V3, the multicast tracking command is ignored.

Examples This example enables tracking and fast leave on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast tracking
```

multicast version

Configures the IGMP version for snooping on a VLAN.

Syntax **multicast version** [**2** | **3**]

no multicast version

Command Default The globally-configured IGMP version is used.

Parameters

2

Configures IGMP version 2.

3

Configures IGMP version 3.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the globally configured version.

If an IGMP version is configured for an individual port, that port uses the version configured for it, not the VLAN version.

See the description of the **ip multicast version** command for information on how to configure the IGMP version globally.

See the description of the **multicast port-version** command for information on how to configure the IGMP version on an individual port

Examples This example configures IGMP version 3 on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast version 3
```

multicast6 disable-mld-snoop

Disables multicast listening discovery (MLD) snooping for a specific VLAN when snooping is enabled globally.

Syntax **multicast6 disable-multicast-snoop**

no multicast6 disable-multicast-snoop

Command Default The global MLD snooping setting applies.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the global MLD snooping setting.

Examples This example disables MLD snooping on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 disable-multicast-snoop
```

multicast6 disable-pimsm-snoop

When PIM6 SM snooping is enabled globally, overrides the global setting and disables it for a specific VLAN.

Syntax **multicast6 disable-pimsm-snoop**

no multicast6 disable-pimsm-snoop

Command Default The globally configured PIM6 SM snooping applies.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the globally configured PIM6 SM snooping.

The device must be in multicast listening discovery (MLD) passive mode before PIM6 SM snooping can be disabled.

Examples This example enables PIM6 SM traffic snooping on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)#multicast6 disable-pimsm-snoop
```

multicast6 fast-convergence

Configures a device to listen to topology change events in Layer 2 protocols such as spanning tree, and then send general queries to shorten the convergence time.

Syntax **multicast6 fast-convergence**

no multicast6 fast-convergence

Command Default Fast convergence is not configured.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default; fast convergence is not configured.

Configure the **multicast6 fast-convergence** command to allow a device to listen to topology change events in Layer 2 protocols, such as Spanning Tree, and send general queries to shorten the convergence time.

If the Layer 2 protocol cannot detect a topology change, fast convergence may not work in some cases. For example, if the direct connection between two devices switches from one interface to another, the Rapid Spanning Tree protocol (802.1w) considers this to be optimization rather than a topology change. In this case, other devices do not receive topology change notifications and cannot send queries to speed up convergence. The original spanning tree protocol does not recognize optimization actions, and fast convergence works in all cases.

Examples This example configures fast convergence on VLAN 70.

```
device# configure terminal
device(config)# vlan 70
device(config-vlan-70)# multicast6 fast-convergence
```

multicast6 port-version

Configures the multicast listening discovery (MLD) version on individual ports in a VLAN.

Syntax **multicast6 port-version** { **1** | **2** } [**ethernet** *stackid|slot|portnum* [**ethernet** *stackid|slot|portnum* | **to** *port*]]

no multicast6 port-version { **1** | **2** } [**ethernet** *stackid|slot|portnum* [**ethernet** *stackid|slot|portnum* | **to** *port*]]

Command Default The port uses the MLD version configured globally or for the VLAN.

Parameters

1

Configures MLD version 1.

2

Configures MLD version 2.

ethernet *stackid|slot|portnum*

Specifies the port to configure the version on. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can specify a list of ports, separated by a space, or a range of ports, or you can combine lists and ranges.

to

Specifies a range of ports.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the MLD version configured globally or for the VLAN.

When you configure the MLD version on a specified port or range of ports, the other ports use the MLD version specified with the **multicast6 version** command, or the globally configured MLD version.

Examples This example configures ports 1/1/4, 1/1/5, 1/1/6, and 1/2/1 on VLAN 20 to use MLD version 2.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 port-version 2 ethernet 1/2/1 ethernet 1/1/4 to
1/1/6
```

multicast6 proxy-off

Turns off multicast listening discovery (MLD) proxy activity.

Syntax **multicast6 proxy-off**

no multicast6 proxy-off

Command Default MLD snooping proxy activity is on.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default; proxy activity is on.

When a device is configured for static groups, it acts as a proxy and sends membership reports for the static groups when it receives general or group-specific queries. When a static group configuration is removed, the group is deleted from the active group table immediately. However, leave messages are not sent to the querier, and the querier must age out the group. You can configure the **multicast proxy-off** command to turn off proxy activity.

Examples This example turns off proxy activity for VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 proxy-off
```

multicast6 router-port

Configures a static router port to receive IPv6 multicast control and data packets.

Syntax **multicast6 router-port ethernet** *stackid|slot|portnum* [**ethernet** *stackid|slot|portnum* | **to** *stackid|slot|portnum*]

no multicast6 router-port ethernet *stackid|slot|portnum* [**ethernet** *stackid|slot|portnum* | **to** *stackid|slot|portnum*]

Command Default The device forwards all IPv6 multicast control and data packets only to router ports that receive queries.

Parameters **ethernet** *stackid|slot|portnum*

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-ID; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID. You can configure a single port or a list of ports, separated by a space.

to

Specifies a range of ports.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default, that is, the device forwards all multicast control and data packets only to router ports that receive queries.

All multicast control and data packets are forwarded to router ports that receive queries. Although router ports are learned, you can configure static router ports to force multicast traffic to specific ports, even though these ports never receive queries.

Examples This example configures a range and a list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast6 router-port ethernet 1/1/1 to 1/1/8 ethernet 1/1/24
ethernet 1/6/24 ethernet 1/8/17
```

multicast6 static-group

Configures a static multicast listening discovery (MLD) group for a VLAN.

Syntax **multicast6 static-group** *ipv6-address* [**count** *num*] [**ethernet** *stackid*/*slot*/*portnum* | **to** *stackid*/*slot*/*portnum*]

no multicast6 static-group *ipv6-address* [**count** *num*] [**ethernet** *stackid*/*slot*/*portnum* | **to** *stackid*/*slot*/*portnum*]

Command Default The VLAN cannot forward multicast traffic to ports that do not receive MLD membership reports.

Parameters *ipv6-address*

Specifies the IPv6 address of the multicast group.

count *num*

Specifies a contiguous range of groups. The default is 1.

to

Specifies a range of ports.

ethernet *stackid*/*slot*/*portnum*

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-ID; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID. You can configure a single port or a list of ports, separated by a space.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command removes the static group fromr the VLAN.

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive MLD membership reports. To allow clients to send reports, you can configure a static group that applies to individual ports on the VLAN. The static group forwards packets to the static group ports even if they have no client membership reports.

You cannot configure a static group that applies to an entire VLAN.

The maximum number of supported static groups in a VLAN is 512, and the maximum number of supported static groups for individual ports in a VLAN is 256.

Examples This example configures on VLAN 20 a static group containing ports 0/1/3 and 0/1/5 to 0/1/7.

```
Device(config)#vlan 20
(config-vlan-20)#multicast6 static-group ff05::100 count 2 ethernet 0/1/3 ethernet
0/1/5 to 0/1/7
```

multicast6 tracking

Enables tracking and fast leave for IPv6 multicast listening discovery Version 2 (MLDv2) on VLANs.

Syntax **multicast6 tracking**

no multicast6 tracking

Command Default Tracking and fast leave are disabled.

Modes VLAN configuration mode

Usage Guidelines The **no** form of this command restores the default, that is, tracking and fast leave are disabled.

The membership tracking and fast leave features are supported for MLDv2 only. If any port or any client is not configured for MLDv2, the multicast tracking command is ignored.

Examples This example enables tracking and fast leave on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 tracking
```

multicast6 version

Configures the multicast listening discovery (MLD) version for snooping on a VLAN.

Syntax **multicast6 version** { **1** | **2** }

no multicast6 version { **1** | **2** }

Command Default The globally configured MLD version is configured.

Parameters **1**

Configures MLD Version 1.

2

Configures MLD Version 2.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the globally configured MLD version.

If an MLD version is specified for individual ports, these ports use that version instead of the version specified for the VLAN.

Examples This example specifies MLD Version 2 on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)#multicast6 version 2
```

nbr-timeout

Configures the interval after which a PIM device considers a neighbor to be absent.

Syntax **nbr-timeout** *seconds*

no nbr-timeout *seconds*

Command Default The timeout interval is 105 seconds.

Parameters *seconds*

Specifies the interval, in seconds. The range is 35 through 65535 seconds. The default is 105 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default timeout interval, 105 seconds.

You should set the interval to be not less than 3.5 times the hello timer value.

Examples This example configures a PIM neighbor timeout value of 360 seconds on all ports on a device operating with PIM.

```
Device(config)# router pim
Device(config-pim-router)# nbr-timeout 360
```

openflow enable

Enables or disables the Openflow hybrid port mode on the port.

Syntax **openflow enable** [**layer2** | **layer3** | **layer23** [**hybrid-mode**]]

no openflow enable [**layer2** | **layer3** | **layer23** [**hybrid-mode**]]

Parameters

layer2

Enables Layer 2 matching mode for flows.

layer3

Enables Layer 3 matching mode for flows.

layer23 hybrid-mode

Enables Layer 2 and Layer 3 matching mode for flows with an option for hybrid port mode.

Modes Interface configuration mode

Usage Guidelines In interface configuration mode, this command enables Layer 2 or Layer 3 matching mode for flows with an optional enabling of hybrid port mode.

NOTE
OpenFlow must be globally enabled before the Layer2 or Layer 3 matching modes can be specified.

Examples After OpenFlow 1.3 is enabled, the following example configures Layer 2 and Layer 3 matching mode for flows.

```
device# configure terminal
device(config)# openflow enable ofv130
device (config)# interface ethernet 1/1/1
device (config-if-1/1/1)# openflow enable layer 23
```

History

Release	Command History
08.0.20	This command was introduced.

originator-id

Configures MSDP to use the specified interface IP address as the IP address of the rendezvous point (RP) in a source-active (SA) message.

Syntax **originator-id** *type number*

no originator-id *type number*

Command Default MSDP uses the IP address of the originating RP in the RP address field of the SA message.

Parameters *type*

Specifies the type of interface used by the RP. You can use Ethernet, loopback, and virtual routing interfaces (ve).

number

Specifies the interface number. For example, the Ethernet port number, loopback number, or virtual routing interface number.

Modes MSDP router configuration mode

MSDP router VRF configuration mode

Usage Guidelines The **no** form of this command restores the default

Examples This example configures an interface IP address to be the IP address of the RP.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ip address 2.2.1.99/32
Device(config)# router msdp
Device(config-msdp-router)# originator-id loopback 2
Device(config-msdp-router)# exit
```

This example configures an interface IP address to be the IP address of the RP on a VRF named blue.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ip address 2.2.1.99/32
Device(config)# router msdp vrf blue
Device(config-msdp-router-vrf blue)# originator-id loopback 2
Device(config-msdp-router-vrf blue)# exit
```

packet-inerror-detect

Enables the monitoring of a port for inError packets and defines the maximum number of inError packets allowed for the port during the configured sampling interval.

Syntax **packet-inerror-detect** *inError-count*

no packet-inerror-detect *inError-count*

Command Default The Packet InError Detect feature is disabled for the port.

Parameters *inError-count*

Specifies the maximum number of inError packets that are allowed for a port during the configured sampling interval. The value can range from 10 through 4294967295.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command disable monitoring of inError packets for the port.

If the number of inError packets received at a port exceeds the default value for two consecutive sampling windows, the port is set to the error-disabled state.

NOTE
To enable monitoring of inError packets for the port only, you must first use the **errdisable packet-inerror-detect** command in global configuration mode to globally enable monitoring for inError packets on the device.

Examples The following example displays the maximum number of allowed inError packets for a port set to the value 10.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# packet-inerror-detect 10
```

History

Release version	Command history
07.3.00g	This command was introduced.

pass-through

Enables pass-through which allows certain protocol packets to pass through ports that have been enabled for flexible authentication.

Syntax **pass-through** { **lldp** | **fdp** | **cdp** }

no pass-through{ **lldp** | **fdp** | **cdp** }

Command Default Pass-through is not enabled.

Parameters

lldp

Specifies the Link Layer Discovery Protocol to pass through.

fdp

Specifies the Foundry Discovery Protocol to pass through.

cdp

Specifies the Cisco Discovery Protocol to pass through.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables pass-through.

This command specifies the protocols to be passed through even though the client is not authenticated.

Examples The example enables LLDP for pass-through.

```
device(config)#authentication
device(config-authen)#pass-through lldp
```

History

Release version	Command history
08.0.20	This command was introduced.

phy cable diagnostics tdr

Runs the VCT TDR test on the specified port.

Syntax **phy cable-diagnostics tdr** *stackid*/*slot*/*port*

Parameters *stackid*/*slot*/*port*

Specifies the interface (port), by device, slot, and port number.

Modes Privileged EXEC mode

Usage Guidelines Use this command to clear TDR test registers before every TDR cable diagnostic test.

Before executing this command, use the **clear cable-diagnostics tdr** command to clear any previous TDR test results.

Display diagnostic test results using the **show cable-diagnostics tdr stackid/slot/port** command.

Examples The following example clears test registers for the interface and then runs the TDR diagnostic test for port 3 on slot 2 of the first device in the stack.

```
device# clear cable-diagnostics tdr 1/2/3
device# phy cable-diag tdr 1/2/3
```

History

Release version	Command history
08.0.20	This command was introduced for ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, and ICX6450-C devices.

prefix-list

Associates an IPv6 prefix list with a Router Advertisement (RA) guard policy.

Syntax **prefix-list** *name*

no prefix-list *name*

Parameters *name*

Specifies the name of the IPv6 prefix list to associate with the RA guard policy.

Modes RA guard policy configuration mode

Usage Guidelines This command associates an IPv6 prefix list with an RA guard policy so that only the RAs that have the given prefix are forwarded. You must provide the name of an IPv6 prefix list already configured using the **ipv6 prefix-list** command. For more information on configuring an IPv6 prefix list using the **ipv6 prefix-list** command, see the *FastIron Ethernet Switch Layer 3 Routing Configuration Guide* .

Only one prefix list can be associated with an RA guard policy. If the command is configured twice with different prefix lists, the latest configured prefix list is associated with the RA guard policy.

Examples The following example associates an IPv6 prefix list with an RA guard policy:

```
Brocade(config)# ipv6 prefix-list raguard-prefix1
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# prefix-list raguard-prefix1
```

pre-shared-key

Configures the pre-shared MACsec key on the interface.

Syntax **pre-shared-key** *key-id* **key-name** *hex-string*

no pre-shared-key *key-id* **key-name** *hex-string*

Command Default No pre-shared MACsec key is configured on the interface.

Parameters *key-id*

Specifies the 32 hexadecimal value used as the Connectivity Association Key (CAK).

key-name *hex-string*

Specifies the 32 hexadecimal characters used as the CAK key name.

Modes dot1x-mka interface mode

Usage Guidelines The **no** form of the command removes the pre-shared key from the interface.

This command is supported only on the Brocade ICX 6610 device.

The pre-shared key is required for communications between MACsec peers.

Examples The following example configures MKA group test1 and assigns the MACsec pre-shared key with a name beginning with 96437a93 and with the value shown, to port 2, slot 3 on the first device in the stack.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# key-server-priority 5
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
device(config-dot1x-mka-group-test1)# exit
device(config-dot1x-mka)# enable-mka ethernet 1/3/2
device(config-dot1x-mka-1/3/2)# mka-group test1
device(config-dot1x-mka-1/3/2)# pre-shared-key 135bd758b0ee5c11c55ff6ab19fdb199 key-
name 96437a93ccf10d9dfe347846cce52c7d
```

History

Release version	Command history
08.0.20	This command was introduced.

priority

Configures a priority value for the device. This value is used along with other factors to determine controller election if a stack failover or merge occurs.

Syntax **priority** *num*

no priority

Command Default The priority value for the active controller and standby device is 128.

Parameters *num*

Possible values are 0 to 255. Lower values assign a lower priority to the device, and higher values assign a higher priority to the device.

Modes Stack unit configuration mode

Usage Guidelines The **no** form of the command restores the default priority value to the device (128). You do not have to specify the default value when using the **no** form.

A unit that has a relatively high priority value is more likely to be elected to be the active controller.

When you change the priority value assigned to a stack unit, the value takes effect immediately but does not affect the active controller until the next reset.

When the active and standby controller have the same priority value, other factors affect controller election, such as up-time and number of members controlled.

Examples The following example assigns a priority value of 130 to stack unit 1.

```
device(Config)# stack unit 1
device(Config-unit-1)# priority 130
```

History

Release version	Command history
08.0.01	This command was introduced.

priority-flow-control

Enables priority flow control (PFC) on a priority group.

Syntax **priority-flow-control** *priority-group-number*

no priority-flow-control *priority-group-number*

Command Default PFC is globally disabled

Parameters *priority-group-number*

Specifies a priority group. The range is 0-3.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default flow-control settings.

To enable global PFC, symmetrical-flow-control must be disabled.

You must enable PFC globally before you configure it for priority groups.

Enabling PFC on a priority group enables PFC on all the ports.

PFC and 802.3x flow control are mutually exclusive. Configuring the **priority-flow-control** command disables 802.3x in both transmit and receive directions.

PFC is not supported for ports across stack units on ICX 7750 devices.

PFC is not supported on ICX 7450 devices.

Examples The following example enables PFC for a priority group:

```
Device(config)# priority-flow-control enable
Device(config)# priority-flow-control 2
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified. Specifying a priority group no longer enables PFC on all ports.

priority-flow-control enable

Enables priority flow control (PFC) globally or on an individual port.

Syntax **priority-flow-control enable**

no priority-flow-control enable

Command Default PFC is disabled (globally and on all ports).

Modes Global configuration mode

Interface configuration mode

Usage Guidelines In global configuration mode, the **no** form of this command restores the default flow-control settings. In interface configuration mode, the **no** form of the command disables PFC on the interface.

To enable global PFC, symmetrical-flow-control must be disabled.

You must enable PFC globally before you configure it for priority groups.

In global configuration mode, configuring the **priority-flow-control enable** command enables PFC globally; in interface configuration mode, configuring it enables PFC on a port. You can configure the **priority-flow-control enable** command in interface configuration mode to enable both PFC transmit and receive, that means PFC is both honored and generated. PFC must be enabled on at least one priority group before you can configure the **priority-flow-control enable** command on an interface.

Priority flow control and 802.3x flow control are mutually exclusive; therefore, configuring the **priority-flow-control enable** command disables 802.3x in both transmit and receive directions.

Examples The following example enables PFC globally.

```
Device(config)# priority-flow-control enable
```

The following example enables PFC on an interface.

```
Device(config-if-e10000-1/1/1)# priority-flow-control enable
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified to add enabling PFC on a port.

prune-timer

Configures the time a PIM device maintains a prune state for a forwarding entry.

Syntax **prune-timer** *seconds*

no prune-timer *seconds*

Command Default The prune time is 180 seconds.

Parameters *seconds*

Specifies the interval in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default prune time, 180 seconds.

The first received multicast interface is forwarded to all other PIM interfaces on the device. If there is no presence of groups on that interface, the leaf node sends a prune message upstream and stores a prune state. This prune state travels up the tree and installs a prune state. A prune state is maintained until the prune timer expires or a graft message is received for the forwarding entry.

Examples This example configures a PIM prune timer to 90 seconds.

```
Device(config)# router pim
Device(config-pim-router)# prune-timer 90
```

prune-wait

Configures the time a PIM device waits before stopping traffic to neighbor devices that do not want the traffic.

Syntax **prune-wait** *seconds*

no prune-wait

Command Default The prune wait time is 3 seconds.

Parameters *seconds*

Specifies the wait time in seconds. The range is 0 through 30 seconds. The default is 3 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the default prune wait time of 3 seconds.

A smaller prune wait value reduces flooding of unwanted traffic. A prune wait value of 0 causes the PIM device to stop traffic immediately upon receiving a prune message.

If there are two or more neighbors on the physical port, you should not configure the **prune-wait** command because one neighbor may send a prune message while the other sends a join message at the same time, or within less than 3 seconds.

Examples This example configures the prune wait time to 0 seconds.

```
Device(config)# router pim
Device(config-pim-router)# prune-wait 0
```

qos egress-buffer-profile

Configures an egress buffer profile.

Syntax **qos egress-buffer-profile** *user-profile-name* **queue-share-level** *level queue-number*

no qos egress-buffer-profile *user-profile-name* **queue-share-level** *level queue-number*

Command Default The egress buffer profile is:

Queue	Share level
0	level4-1/9
1	level3-1/16
2	level3-1/16
3	level3-1/16
4	level3-1/16
5	level3-1/16
6	level3-1/16
7	level3-1/16

Parameters *user-profile-name*

Specifies the name of the egress buffer profile to be configured.

queue-share-level *level*

Specifies the number of buffers that can be used in a sharing pool. Eight levels are supported.

queue-number

Specifies the queue to apply the buffer limit to. There are eight hardware queues per port.

Modes Global configuration mode

Usage Guidelines The **no** form of this command deletes the egress buffer profile.

You can attach an egress buffer profile to a port.

You must configure the **no qos egress-buffer-profile** command to detach a profile from any ports that are using it before you can configure the **no qos egress-buffer-profile** command to delete it.

The higher the sharing level, the better the port absorb micro-burst. However, higher-sharing levels of 7 and 8 may compromise QoS functions and create uneven distribution of traffic during periods of congestion.

The following eight queue-share levels are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool
level6-1/3	1/3 of buffers in the sharing pool
level7-1/2	1/2 of buffers in the sharing pool
level8-2/3	2/3 of buffers in the sharing pool

Examples

The following example creates an egress buffer profile named port-40G.

```
Device(config)# qos egress-buffer-profile port-40G queue-share-level
  level1-1/64   1/64 of buffers in the sharing pool
  level2-1/32   1/32 of buffers in the sharing pool
  level3-1/16   1/16 of buffers in the sharing pool
  level4-1/9    1/9 of buffers in the sharing pool
  level5-1/5    1/5 of buffers in the sharing pool
  level6-1/3    1/3 of buffers in the sharing pool
  level7-1/2    1/2 of buffers in the sharing pool
  level8-2/3    2/3 buffers in the sharing pool
```

The following example configures queue 0 on the egress buffer profile named port-40G to use 1/5 of sharing pool.

```
Device(config)# qos egress-buffer-profile port-40G port-40G queue-share-level
level5-1/5 0
```

The following example configures queue 1 on the egress buffer profile named port-40G to use 1/64 of the sharing pool.

```
Device(config)# qos egress-buffer-profile port-40G port-40G queue-share-level
level1-1/64 1
```

The following example attaches the egress buffer profile named port-40G to ports 1/2/1 to 1/2/6.

```
Device(config)# interface ethernet 1/2/1 to 1/2/6
Device(config-mif-1/2/1-1/2/6)#egress-buffer-profile port-40G
Device(config-mif-1/2/1-1/2/6)#end
```

The following example shows the error if you try to delete a profile that is attached to a port.

```
Device(config)# no qos egress-buffer-profile port-40G
Error - Egress Profile port-40G is active on Port 1/2/1. It must be deactivated from
port before deleting.
```

The following example detaches the egress buffer profile named port-40G from ports 1/2/1 to 1/2/6 and then delete the profile.

```
Device(config)# interface ethernet 1/2/1 to 1/2/6
Device(config-mif-1/2/1-1/2/6)# no egress-buffer-profile port-40G
Device(config-mif-1/2/1-1/2/6)#exit
Device(config)# no qos egress-buffer-profile port-40G
```

History

Release version	Command history
8.0.10	This command was introduced.

qos ingress-buffer-profile

Configures an ingress buffer profile.

Syntax **qos ingress-buffer-profile** *user-profile-name* **priority-group** *priority-group-number* **xoff** *shared-level*

no qos ingress-buffer-profile *user-profile-name* **priority-group** *priority-group-number* **xoff** *shared-level*

Command Default An ingress buffer profile is not configured.

Parameters *user-profile-name*

Specifies the name of the ingress buffer profile to be configured.

priority-group *priority-group-number*

Specifies the priority group (PG) number whose XOFF threshold level has to be configured.

xoff *shared-level*

Specifies the per-PG buffer threshold to trigger sending of priority flow control (PFC).

Modes Global configuration mode

Usage Guidelines The **no** form of this command deletes the ingress buffer profile.

You can attach an ingress buffer profile to a port.

You must configure the **no qos ingress-buffer-profile** command to detach a profile from any ports that are using it before you can configure the **no qos ingress-buffer-profile** command to delete it.

The higher the sharing level, the better the port absorbs micro-bursts, before reaching the XOFF threshold limit.

If PFC is enabled on PG and per-port with a user-defined ingress buffer profile attached to a port, port max XOFF is 50% of service pool 1. Port max is used as a cap to prevent a port from using too many buffers. Under normal conditions, the PG XOFF limit is reached first.

If a PG is not enabled to send globally, any XOFF value configured has no effect.

The default ingress buffer profiles are as follows:

- For PFC disabled ports, the default PG XOFF limit is level7-1/2
- For PFC enabled ports, the default PG XOFF limit is level2-1/32

The following six PG XOFF limits are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool

Level	Sharing-pool buffers
level6-1/3	1/3 of buffers in the sharing pool

Examples

The following example creates an ingress buffer profile for PG 0 with a PG XOFF limit of 1/3 of buffers in the sharing pool.

```
Device(config)#qos ingress-buffer-profile ing1 priority-group 0 xoff level6-1/3
```

History

Release version	Command history
8.0.20	This command was introduced.

qos priority-to-pg

Configures priority-to-priority-group (PG) mapping for priority flow control (PFC).

Syntax **qos priority-to-pg qosp0** *priority-PG-map* **qosp1** *priority-PG-map* **qosp2** *priority-PG-map* **qosp3** *priority-PG-map* **qosp4** *priority-PG-map* **qosp5** *priority-PG-map* **qosp6** *priority-PG-map* **qosp7** *priority-PG-map*

no qos priority-to-pg

Command Default Priority-to-PG mapping is not configured.

Parameters

qosp0-7

Configures the internal priority based on classification in the range 0 through 7.

priority-PG-map

Specifies the internal priority-to-PG mapping. The range is 0 through 3.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default priority-to-PG map.

You must configure the **priority-flow-control enable** command to enable PFC globally before you configure priority-to-PG mapping.

NOTE

Default mapping, mapping priorities, and mapping restrictions changed in Brocade FastIron Release 8.0.20. The following restrictions apply:

- Priority 7, and only Priority 7, is always mapped to PG4.
- PG4 is always lossy.
- PFC cannot be enabled on PG4.
- Priorities 0 to 5 can be mapped to PG0, PG1, and PG2. They cannot be mapped to PG3 or PG4.

The default value of priority-to-PG maps is:

- QoS internal priority 0 is mapped to PG 0
- QoS internal priority 1 is mapped to PG 0
- QoS internal priority 2 is mapped to PG 1
- QoS internal priority 3 is mapped to PG 1
- QoS internal priority 4 is mapped to PG 1
- QoS internal priority 5 is mapped to PG 2
- QoS internal priority 6 is mapped to PG 2
- QoS internal priority 7 is mapped to PG 4

The default value of priority-to-PG maps in releases prior to Release 8.0.20 is:

- QoS internal priority 0 is mapped to PG 0
- QoS internal priority 1 is mapped to PG 0
- QoS internal priority 2 is mapped to PG 1
- QoS internal priority 3 is mapped to PG 1
- QoS internal priority 4 is mapped to PG 1
- QoS internal priority 5 is mapped to PG 2

- QoS internal priority 6 is mapped to PG 2
- QoS internal priority 7 is mapped to PG 2

In releases prior to Release 8.0.20, you can map QoS internal priority 7 to PG 3. You can also map any other priority to PG 3 if it meets these requirements:

- Lower priorities mapped to lower PGs.
- PGs are configured in ascending order.
- Multiple priorities in a single PG must be consecutive.

Priority-to-PG mapping is not configurable in other modes. Symmetrical and asymmetrical 802.3x flow control modes have their own default priority-to-PG mapping.

You must configure PGs in ascending order, 0 to 3. You can configure a higher-order PG only if all the lower-order PGs have some mapped priorities.

Examples

The following example configures a priority-to-PG map.

```
Device(config)# priority-flow-control enable
Device(config)# qos priority-to-pg qosp0 0 qosp1 1 qosp2 1 qosp3 1 qosp4 2 qosp5 2
qosp6 2 qosp7 4
```

The following example restores the default priority-to-PG map.

```
Device(config)# no qos priority-to-pg qosp0 0 qosp1 1 qosp2 1 qosp3 1 qosp4 2 qosp5 2
qosp6 2 qosp7 4
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified to change priority 7-to-PG4 mapping and mapping restrictions for priorities 0 through 5.

qos scheduler-profile

Configures a user-defined Quality of Service (QoS) scheduler profile.

Syntax **qos scheduler-profile** *user-profile-name* { **mechanism** *scheduling-mechanism* | **profile** [**qosp0** *wt0* | **qosp1** *wt1* | **qosp2** *wt2* | **qosp3** *wt3* | **qosp4** *wt4* | **qosp5** *wt5* | **qosp6** *wt6* | **qosp7** *wt7*] }

no qos scheduler-profile *user-profile-name*

Command Default A user-defined QoS scheduler profile is not configured.

Parameters *user-profile-name*

Specifies the name of the scheduler profile to be configured.

mechanism *scheduling-mechanism*

Configures the queue assignment with the specified scheduling mechanism. The following scheduling mechanisms are supported:

mixed-sp-wrr

Specifies mixed strict-priority (SP) and weighted scheduling.

strict

Specifies SP scheduling.

weighted

Specifies weighted scheduling.

profile qosp0-7

Configures the profile based on classification in the range 0 through 7.

wt0-7

Specifies the bandwidth percentage for the corresponding QoS profile. The range is from 0 through 7.

Modes Global configuration mode

Usage Guidelines The **no** form of this command removes the scheduler profile configuration.

You can use the **scheduler-profile** command to attach a user scheduler profile to a port. If you want to remove a scheduler-profile you must ensure that it is not attached to any port.

On ICX 7750 and ICX 7450 devices, changing the global scheduler and port scheduler on running traffic may cause traffic loss.

The default QoS-profile weights for each queue using a weighted QoS mechanism are as follows:

Profile	Priority	Weighted bandwidth
Profile qosp7	Priority7(Highest)	Bandwidth requested 44% calculated 44%
Profile qosp6	Priority6	Bandwidth requested 8% calculated 8%
Profile qosp5	Priority5	Bandwidth requested 8% calculated 8%
Profile qosp4	Priority4	Bandwidth requested 8% calculated 8%
Profile qosp3	Priority3	Bandwidth requested 8% calculated 8%
Profile qos2	Priority2	Bandwidth requested 8% calculated 8%
Profile qosp1	Priority1	Bandwidth requested 8% calculated 8%
Profile qosp0	Priority0 (Lowest)	Bandwidth requested 8% calculated 8%

Per-queue details	Bandwidth percentage
Class 0	3
Class 1	3
Class 2	3
Class 3	3
Class 4	3
Class 5	3
Class 6	7
Class 7	75

The default QoS-profile weights for each queue using a mixed QoS mechanism are as follows:

Per-queue details	Bandwidth percentage
Class 0	15
Class 1	15
Class 2	15
Class 3	15
Class 4	15
Class 5	25
Class 6	sp
Class 7	sp

The total weight (wt0-wt7) in both weighted and mixed mechanism must be 100 percent.

The minimum value for any weight is 1.

A maximum of eight scheduler profiles are supported.

Examples The following example configures a QoS scheduler profile named user1, with weighted scheduling, and specify the bandwidth percentage for each QoS class:.

```
Device(config)# qos scheduler-profile user1 mechanism weighted
Device(config)# qos scheduler-profile user1 profile qosp0 1 qosp1 1 qosp2 10 qosp3 10
qosp4 10 qosp5 10 qosp6 20 qosp7 38
```

The following example configures a QoS scheduler profile named user2, with SP scheduling.

```
Device(config)# qos scheduler-profile user2 mechanism strict
```

The following example configures a QoS scheduler profile named user3, with mixed SP and weighted scheduling.

```
Device(config)# qos scheduler-profile user3 mechanism mixed-sp-wrr
```

The following example removes a QoS scheduler profile named user3.

```
Device(config)# no qos scheduler-profile user3
```

History

Release version	Command history
08.0.10	This command was introduced.

qos-internal-trunk-queue

Modifies the dynamic buffer-share level of inter-packet-processor (inter-pp) HiGig links egress queues on ICX 7450 devices.

Syntax **qos-internal-trunk-queue** *level queue*

no qos-internal-trunk-queue *level queue*

Command Default The buffer share level defaults are:

Queue	Share level
0	level4-1/9
1	level3-1/16
2	level3-1/16
3	level3-1/16
4	level3-1/16
5	level3-1/16
6	level3-1/16
7	level3-1/16

Parameters *level*

Specifies the number of buffers that can be used in a sharing pool. ICX 7450 devices support eight levels.

queue

Specifies the queue to apply the buffer limit to. Each port has eight hardware queues.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default queue share level on the specified queue.

NOTE
This command is supported only on ICX 7450 devices or across stack units or for ports across master and slave packet-processor (pp) devices in ICX7450-48 units.

The following eight queue-share levels are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool

Level	Sharing-pool buffers
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool
level6-1/3	1/3 of buffers in the sharing pool
level7-1/2	1/2 of buffers in the sharing pool
level8-2/3	2/3 of buffers in the sharing pool

Examples

The following example configures the buffer share level of inter-packet-processor (inter-pp) HiGig links egress queues.

```
ICX7450-48P Router(config)#qos-internal-trunk-queue
  level1-1/64   1/64 of buffers in the sharing pool
  level2-1/32   1/32 of buffers in the sharing pool
  level3-1/16   1/16 of buffers in the sharing pool
  level4-1/9    1/9 of buffers in the sharing pool
  level5-1/5    1/5 of buffers in the sharing pool
  level6-1/3    1/3 of buffers in the sharing pool
  level7-1/2    1/2 of buffers in the sharing pool
  level8-2/3    2/3 buffers in the sharing pool
```

History

Release version	Command history
08.0.20	This command was introduced.

radius-client coa host

Configures the key to be used between the Change of Authorization (CoA) client and FastIron device.

Syntax **radius-client coa host** { *addr* | *name* } [**key** *key-string*]

no radius-client coa host { *addr* | *name* } [**key** *key-string*]

Command Default No key is configured between the CoA client and device.

Parameters

addr
Address of the CoA host.

name
Name of the CoA host.

key *key-string*
The key required to be used between the CoA client and FastIron device.

Modes Global configuration mode

Usage Guidelines RADIUS Change of Authorization (CoA) messages from clients configured through this command will be processed. CoA messages from unconfigured clients will be discarded.

Examples The following example displays the configuration between CoA host and the device.

```
device(config)# radius-client coa host 10.21.240.46 key 0 Foundry1#
```

History

Release version	Command history
08.0.20	This command was introduced.

radius-client coa port

Changes the default CoA (Change of Authorization) port number.

Syntax **radius-client coa port** *udp-port-number*

no radius-client coa port *udp-port-number*

Command Default The CoA port number is 3799.

Parameters *udp-port-number*

The number of the UDP port.

Modes Global configuration mode

Usage Guidelines The **no** form of the command restores the default port number (3799).

Examples The following example changes the CoA port number to 3000.

```
device(config)# radius-client coa port 3000
```

History

Release version	Command history
08.0.20	This command was introduced.

raguard

Configures the current interface as a trusted, untrusted, or host Router Advertisement (RA) guard port.

Syntax **raguard** { **trust** | **untrust** | **host** }

no raguard { **trust** | **untrust** | **host** }

Parameters

trust

Configures an interface as a trusted RA guard port.

untrust

Configures an interface as an untrusted RA guard port.

host

Configures an interface as a host RA guard port.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command removes the current trusted or untrusted configuration.

A trusted RA guard port forwards all the receive RA packets without inspecting. An untrusted port inspects the received RAs against the RA guard policy's whitelist, prefix list and preference maximum settings before forwarding the RA packets. If an RA guard policy is not configured on an untrusted or host port, all the RA packets are forwarded.

Examples The following example configures an interface as a trusted RA guard port:

```
Brocade(config)# interface ethernet1/1/1
Brocade(config-int-e1000-1/1/1)# raguard trust
```

The following example configures an interface as an untrusted RA guard port:

```
Brocade(config)# interface ethernet1/2/1
Brocade(config-int-e1000-1/2/1)# raguard untrust
```

The following example configures an interface as a host RA guard port:

```
Brocade(config)# interface ethernet3/2/1
Brocade(config-int-e1000-3/2/1)# raguard host
```

register-probe-time

Configures the time the PIM router waits for a register-stop from a rendezvous point (RP) before it generates another NULL register to the PIM RP

Syntax **register-probe-time** *seconds*

no register-probe-time *seconds*

Command Default The wait time is10 seconds.

Parameters *seconds*

Specifies the time, in seconds, between queries. The range is 10 through 50 seconds. The default is 10 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the wait time to 10 seconds.

The register-probe time configuration applies only to the first-hop PIM router.

NOTE
When a PIM first-hop router has successfully registered with a PIM RP, the PIM first-hop router will not default back to the data registration. All subsequent registers will be in the form of the NULL registration.

Examples This example configures the register-probe time to 20 seconds.

```
Device(config)#router pim
Device(config-pim-router)#register-probe-time 20
```

register-suppress-time

Configures the interval at which the PIM router triggers the NULL register message.

Syntax **register-suppress-time** *seconds*

no register-suppress-time *seconds*

Command Default The interval at which PIM router triggers the NULL register message is 60 seconds.

Parameters *seconds*

Specifies the interval, in seconds, between queries. The range is 60 through 120 seconds. The default is 60 seconds.

Modes PIM router configuration mode

Usage Guidelines The **no** form of this command restores the register-suppress interval to 60 seconds.

The register-suppress interval configuration applies only to the first-hop PIM router.

Examples The following example configures the interval at which PIM router triggers the NULL register message to 90 seconds.

```
Device(config)#router pim
Device(config-pim-router)#register-suppress-time 90
```

restricted-vlan

Configures the restricted VLAN at the global level.

Syntax **restricted-vlan** *vlan-id*

no restricted-vlan *vlan-id*

Command Default The restricted VLAN is not specified.

Parameters *vlan-id*

Specifies the identification number of the restricted VLAN.

Modes Authentication mode

Usage Guidelines The **no** form of the command disables the restricted VLAN.

Use this command to move the port to a restricted VLAN when multi-device port authentication fails.

Examples The following example creates a restricted VLAN with VLAN 1.

```
device(config)# authentication
device(config-authen)# restricted-vlan 1
```

History

Release version	Command history
08.0.20	This command was introduced.

route-precedence

Configures a table that defines the order (precedence) in which multicast routes are selected from the multicast routing table (mRTM) and unicast routing (uRTM) table.

Syntax **route-precedence** { [**mc-non-default** | **none**] | [**mc-default** | **none**] | [**uc-non-default** | **none**] | [**uc-default** | **none**] }

no route-precedence

Command Default The default route precedence used to select routes is:

1. A non-default multicast route from the mRTM (**mc-non-default**).
2. A default multicast route from the mRTM (**mc-default**).
3. A non-default unicast route from the uRTM (**uc-non-default**).
4. A default unicast route from the uRTM (**uc-non-default**).

Parameters

mc-non-default
Specifies the precedence for the non-default multicast route table (mRTM).

none
Specifies that this type of route is to be ignored. You can specify this option for any of the multicast or unicast route types.

mc-default
Specifies the precedence for the multicast routing table (mRTM).

uc-non-default
Specifies the precedence for the non-default unicast route table (uRTM).

uc-default
Specifies the precedence for the default unicast route table (uRTM).

Modes PIM configuration mode

Usage Guidelines The order in which you place the keywords determines the route precedence.

The **no** form of this command restores the default route precedence settings.

You must configure four parameters indicating the four different route types. If you want to specify that a particular route type is not used, configure the **none** keyword to fill the precedence table.

Examples The following example configures a route precedence in which a non-default multicast route has the highest precedence, and a default unicast route has the lowest precedence. The order used to select routes is:

1. A non-default multicast route from the mRTM.
2. A non-default unicast route from the uRTM.
3. A default multicast route from the mRTM.
4. A default unicast route from the uRTM

```
Device(config)# router pim
Device(config-pim-router)# route-precedence mc-non-default uc-non-default mc-default
uc-default
```

The following example configures a route precedence in which the unicast default route is ignored. The order used to select routes is:

1. A non-default multicast route from the mRTM.
2. A default multicast route from the mRTM.
3. A non-default unicast route from the uRTM.

```
Device(config)# router pim
Device(config-pim-router)# route-precedence mc-non-default mc-default uc-non-default
none
```

History

Release version	Command history
8.0.10a	This command was introduced.

route-precedence admin-distance

Configures route precedence so that multicast routes are selected from the best route in the multicast routing table (mRTM) and unicast routing (uRTM) table.

Syntax

route-precedence admin-distance

no route-precedence admin-distance

Command Default

Multicast routes are not selected from the best route in the mRTM and uRTM. Routes are selected based on:

- The route precedence configured using the **route-precedence** command.
- The system route precedence default (if route precedence has not been configured using the **route-precedence** command.

the default route precedence settings.

Modes

PIM configuration mode

Usage Guidelines

The **no** form of this command restores the previous route precedence settings.

If the mRTM and the uRTM have routes of equal cost, the route from the mRTM is preferred.

Examples

The following example configures route precedence so that the best multicast route from the mRTM and uRTM tables is selected.

```
Device(config)#router pim
Device(config-pim-router)#route-precedence admin-distance
```

History

Release version	Command history
8.0.10a	This command was introduced.

router msdp

Enables multicast source discovery protocol (MSDP) on a router.

Syntax **router msdp** [**vrf** *vrf-name*]

Command Default MSDP is not enabled.

Parameters **vrf** *vrf-name*

Specifies a virtual routing and forwarding (VRF) instance.

Modes Global configuration mode

Usage Guidelines When you configure the **no router msdp vrf** *vrf-name* command, the MSDP configuration is removed only from the specified VRF.

The PIM Sparse Rendezvous Point (RP) is also an MSDP peer.

Devices that run MSDP usually also run BGP. The source address used by the MSDP device is normally configured to be the same source address used by BGP.

All MSDP parameters available for the default router instance are configurable for a VRF-based MSDP instance.

Examples The following example enables MSDP.

```
Device(config)# router msdp
```

The following example enables MSDP on a VRF named blue.

```
Device(config)# router msdp vrf blue
```

The following example removes the MSDP configuration only from the VRF named blue.

```
Device(config-msdp-router-vrf-blue)# no router msdp vrf blue
```

router pim

Configures basic global protocol-independent multicast (PIM) Sparse parameters on a device within the PIM Sparse domain and enters PIM-router configuration mode.

Syntax **router pim** [**vrf** *vrf-name*]

no router pim [**vrf** *vrf-name*]

Command Default PIM Sparse is not configured.

Parameters **vrf** *vrf-name*

Specifies a virtual routing and forwarding (VRF) instance.

Modes Global configuration mode

Interface configuration mode

Usage Guidelines The **no** form of this command disables PIM and removes all configuration for PIM multicast on the device (**router pim** level) only. Configuring the **no router pim vrf** *vrf-name* command removes all configuration for PIM multicast on the specified VRF.

You do not need to globally enable IP multicast routing when configuring PIM Sparse.

After you enable IP multicast routing and PIM Sparse at the global level, you must enable it on the individual interfaces connected to the PIM Sparse network.

If you configure PIM Sparse on an interface that is on the border of the PIM Sparse domain, you also must also configure the **ip pim border** command on the interface.

You must configure the **bsr-candidate ethernet** command to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse Rendezvous Point (RP).

You can configure the **rp-address** command to explicitly identify an RP, including an ACL-based RP, by its IP address instead of having it identified by the RP election process.

Entering the **router pim vrf** command to enable PIM does not require a software reload.

All PIM parameters available for the default router instance are configurable for a VRF-based PIM instance.

Examples This example configures basic global PIM Sparse parameters.

```
Device(config)# router pim
```

This example configures PIM Sparse on a VRF named blue.

```
Device(config)# router pim blue
```

rp-address

Configures a device interface as a rendezvous point (RP).

Syntax **rp-address** { *ip-address* | *ipv6-address* } *acl_name_or_id*

no rp-address { *ip-address* | *ipv6-address* }

Command Default The RP is selected by the PIM Sparse protocol's RP election process.

Parameters *ip-address*

Specifies the IP address of the RP.

ipv6-address

Specifies the IPv6 address of the RP.

acl_name_or_id

Specifies the name or ID of the ACL that specifies which multicast groups use the RP.

Modes Router configuration mode

VRF configuration mode

Usage Guidelines The **no** form of this command restores the default and the RP is selected by the RP election process.

Devices in the PIM Sparse domain use the specified RP and ignore group-to-RP mappings received from the bootstrap router (BSR).

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the PIM Sparse routers.

NOTE
Specify the same IP or IPv6 address as the RP on all PIM Sparse devices within the PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network.

Examples This example configures the device interface at IP address 207.95.7.1 as the RP for the PIM Sparse domain.

```
Device(config)# router pim
Device(config-pim-router)# rp-address 207.95.7.1
```

This example configures an ACL named acl1 to specify which multicast groups use the RP.

```
Device(config)# router pim
Device(config-pim-router)# rp-address 130.1.1.1 acl1
```

This example configures an RP for a VRF named blue.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# rp-address 31::207
```

rp-adv-interval

Configures the interval at which the candidate rendezvous point (RP) configured on the device sends candidate-RP advertisement messages to the bootstrap router (BSR).

Syntax **rp-adv-interval** *seconds*

no rp-adv-interval *seconds*

Command Default The device sends candidate-RP advertisement messages every 60 seconds.

Parameters *seconds*

Specifies the interval, in seconds, between advertisement messages. The range is 10 through 65535 seconds. The default is 60 seconds.

Modes PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines The **no** form of this command restores the candidate-RP advertisement-message interval to 60 seconds.

Examples The following example configures the candidate-RP advertisement-message interval to 90 seconds.

```
Device(config)#router pim
Device(config-pim-router)#rp-adv-interval 90
```

The following example configures, on a VRF named blue, the candidate-RP advertisement-message interval to 90 seconds.

```
Device(config)#ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)#rp-adv-interval 90
```

rp-candidate

Configures a device as a candidate rendezvous point (RP) for all multicast groups with the prefix 224.0.0.0/4, by default, and explicitly adds or deletes groups with other prefixes.

Syntax **rp-candidate** { **ethernet** *stackid / slot / portnum* | **loopback** *num* | **ve** *num* | **tunnel** *num* }

rp-candidate {**add** | **delete** } *group-addr mask-bits*

no rp-candidate { **ethernet** *stackid / slot / portnum* | **loopback** *num* | **ve** *num* | **tunnel** *num* }

no rp-candidate {**add** | **delete** } *group-addr mask-bits*

Command Default The PIM router is not available for selection as an RP.

Parameters

ethernet *stackid/slot/portnum*

Specifies a physical interface for the candidate RP. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *num*

Specifies a loopback interface for the candidate RP.

ve *num*

Specifies a virtual interface for the candidate RP.

tunnel *num*

Specifies a GRE tunnel interface for the candidate RP.

add

Specifies adding a group address or range of group addresses to the default group configured by the those the device is the candidate RP for by default, that is, groups with the prefix 224.0.0.0/4.

delete

Specifies deleting a group address or range of group addresses, that were added using the **add** keyword.

group-addr mask-bits

Specifies the group address and the number of significant bits in the subnet mask.

Modes Router PIM configuration mode

Usage Guidelines The **no rp-candidate** command makes the PIM router cease to act as a candidate RP.

The **no rp-candidate add** command deletes a group address or range of group addresses that were added using the **add** keyword.

Configuring the **rp-candidate** command on an Ethernet, loopback, virtual, or tunnel interface, configures the device as a candidate RP for all multicast groups with the prefix 224.0.0.0/4, by default. You can configure the **rp-candidate add** command to add to those a group address or range of group addresses. You can configure the **rp-candidate delete** command to delete a group address or range of group addresses that were added to the default addresses.

NOTE
You cannot delete the default group prefix.

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse

routers learn the addresses of RPs and the groups for which they are responsible from messages that the bootstrap router (BSR) sends to each of the PIM Sparse routers.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

NOTE
Specify the same IPv6 address as the RP on all IPv6 PIM Sparse routers within the IPv6 PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network. You can configure the **rp-address** command to specify the RP address.

Examples

This example configures a physical device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ethernet 1/2/2
```

This example uses a loopback interface to configure a device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate loopback 1
```

This example uses a virtual interface to configure a device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ve 120
```

This example configures an address group to the devices for which it is a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate add 224.126.0.0 16
```

This example deletes an address group from the devices for which it is a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate delete 224.126.22.0 24
```

History

Release version	Command history
8.0.20	This command was modified to add the **tunnel** keyword.

rp-embedded

Configures embedded-rendezvous point (RP) support on PIM devices.

Syntax **rp-embedded**

no rp-embedded

Command Default Embedded RP support is enabled.

Modes PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines The **no** form of this command disables embedded RP support.

Examples This example disables embedded RP support.

```
Device(config)# ipv6 router pim
Device(config-ipv6-pim-router)#no rp-embedded
```

This example disables embedded RP support on a VRF named blue.

```
Device(config)#ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)#no rp-embedded
```

scheduler-profile

Attaches a scheduler profile to one or more ports.

Syntax **scheduler-profile** *profile-name*

no scheduler-profile *profile-name*

Command Default A scheduler profile is not attached to a port.

Parameters *profile-name*

Specifies the name of the scheduler profile to be attached to the port.

Modes Interface mode

Multiple-interface mode

Usage Guidelines The **no** form of this command removes the scheduler profile from the port or ports.

You must configure a user scheduler profile before you can attach it to a port.

Only one scheduler profile at a time can be attached to any port. You can attach a scheduler profile to more than one port.

Examples The following example attaches a scheduler profile named user1 to a port.

```
Device(config-if-e10000-1/1/1)# scheduler-profile user1
```

The following example attaches a scheduler profile named user2 to multiple ports.

```
Device(config-mif-1/1/2-1/1/16)# scheduler-profile user2
```

The following example removes a scheduler profile named user2 from multiple ports.

```
Device(config-mif-1/1/2-1/1/16)# no scheduler-profile user2
```

History

Release version	Command history
8.0.10	This command was introduced.

Show Commands

show cable-diagnostics tdr

Displays the results of Virtual Cable Test (VCT) TDR cable diagnostic testing.

Syntax **show cable-diagnostics tdr** *stackid*/*slot*/ *port*

Parameters ***stackid*/*slot*/*port***

Identifies the specific interface (port), by device, slot, and port number in the format shown.

Modes User EXEC mode

Privileged EXEC mode

Usage Guidelines Most Brocade devices support VCT technology. VCT technology enables the diagnosis of a conductor (wire or cable) by sending a pulsed signal into the conductor, then examining the reflection of that pulse. This method of cable analysis is referred to as Time Domain Reflectometry (TDR). By examining the reflection, the Brocade device can detect and report cable statistics such as local and remote link pair, cable length, and link status.

THis command is supported only on the Brocade ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, and ICX6450-C.

Examples The following example displays TDR test results for port 1, slot 2 on device 3 in the stack. The results indicate that the port is down or the cable is not connected.

```
device>show cable-diagnostics tdr 3/2/1

Port      Speed Local pair Pair Length Remote pair Pair status
--------- ----- ---------- ----------- ----------- -----------
01        UNKWN Pair A     >=3 M                   Open
                Pair B     >=3 M                   Open
                Pair C     >=3 M                   Open
                Pair D     >=3 M                   Open
```

The following example displays I the TDR test results for the same port show details for an active port.

```
device>show cable-diagnostics tdr 3/2/1

Port      Speed Local pair Pair Length Remote pair Pair status
--------- ----- ---------- ----------- ----------- -----------
01        1000M Pair A     50M         Pair B      Terminated
                Pair B     50M         Pair A      Terminated
                Pair C     50M         Pair D      Terminated
                Pair D     50M         Pair C      Terminated
```

History

Release version	Command history
08.0.20	This command was introduced.

show default values

Displays default, maximum, current, and configured values for system maximum parameters.

Syntax **show default values**

Modes Privileged EXEC mode

Examples This example does not show complete output; it shows only PIM hardware mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
pim-hw-mcache         1024       6144       1500       1500
```

This example does not show complete output; it shows only PIM6 hardware mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
pim6-hw-mcache        512        1024       1024       1024
```

This example does not show complete output; it shows only MLD mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
mld-snoop-mcache      512        8192       512        512
```

This example does not show complete output; it shows only IGMP group values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
igmp-snoop-group-add  4096       8192       5000       5000
```

This example does not show complete output; it shows only MLD group values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
MLD-snoop-group-addr  4096       8192       5000       5000
```

show dlb-internal-trunk-hash

Displays the dynamic load balancing (DLB) hashing method for inter-packet-processor (inter-pp) links that connect master and slave units in ICX 7450-48 devices.

Syntax **show dlb-internal-trunk-hash**

Modes Global configuration mode

Examples The following example displays the hashing method in effect for inter-pp links on an ICX 7450-48 device.

```
ICX7450-48P Router(config)#show dlb-internal-trunk-hash
Internal trunk mode: spray-mode
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x ip-acl

Displays the layer 3 ACLs for dot1x authentication.

Syntax **show dot1x ip-acl** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters **all**

Specifies the ACLs at the global level.

ethernet *device*/*slot*/*port*

Specifies the ACLs at the interface level.

Modes Privileged EXEC mode

Examples The following example displays dot1x IP ACL authentication information for all interfaces.

```
device# show dot1x ip-acl all

802.1X IP ACL Information :

Port 2/1/2 : 0013.9400.0002
In-bound IP ACL : 123

Port 2/1/2 : 0013.9400.0001
In-bound IP ACL : 123
```

The following example displays dot1x IP ACL authentication information for Ethernet interface 2/1/2.

```
device# show dot1x ip-acl ethernet 2/1/2

802.1X IP ACL Information :

Port 2/1/2 : 0013.9400.0002
In-bound IP ACL : 123

Port 2/1/2 : 0013.9400.0001
In-bound IP ACL : 123
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x mac-filter

Shows the layer 2 ACLs for dot1x authentication.

Syntax **show dot1x mac-filter** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters **all**

Specifies the ACLs at the global level.

ethernet *device*/*slot*/*port*

Specifies the ACLs at the interface level.

Modes Global configuration

Interface configuration

Command Output The **show mac-filter** command displays the following information:

Output field	Description
Dynamic MAC filter-list	The MAC filter defined on the device.

Examples The **show dot1x mac-filter** command displays the following information

```
device# show dot1x mac-filter all
802.1x MAC Address Filter information:
Port 1/1/48:
Dynamic MAC filter-list: 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x sessions

Shows dot1x configuration sessions at the global and interface level.

Syntax **show dot1x sessions** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters **all**

Specifies the sessions at the global level.

ethernet*device*/*slot*/*port*

Specifies the sessions at the interface level.

Modes Global configuration

Interface configuration

Command Output The **show dot1x sessions** command displays the following information:

Output field	Description
Port	The port number.
MAC Address	The MAC address of the client.
IP Address	The IP address of the client.
VLAN	The VLAN
Auth State	The authentication state.
ACL	The specific ACL applied.
Age	The age of the session.
PAE State	The Port Access Entity state.

Examples The **show dot1x sessions** command displays the following information:

```
device# show dot1x sessions all
Port      MAC             IP              User         Vlan   Auth       ACL   Age
PAE
          Addr            Addr            Name                State
State
-------------------------------------------------------------------------------
------
1/1/1  0024.3821.48dd  N/A             N/A             4092 init    none    S36734
CONNECTING
1/1/2  748e.f8b7.8f61  N/A             N/A             200  init    none    Ena   HELD



device# show dot1x sessions ethernet 1/1/15
-------------------------------------------------------------------------------
------

Port      MAC             IP              User         Vlan   Auth       ACL   Age
PAE
          Addr            Addr            Name                State
State
-------------------------------------------------------------------------------
------
1/1/1  0024.3821.48dd  N/A             N/A             4092 init    none    S36750
CONNECTING
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x statistics

Displays the 802.1x (dot1x) authentication statistics.

Syntax **show dot1x statistics** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters **all**

Displays the dot1x authentication statistics for all interfaces.

ethernet *device*/*slot*/*port*

Displays the dot1x authentication statistics for the specified interface.

Modes Privileged EXEC mode

Command Output The **show dot1x statistics** command displays the following information:

Output field	Description
RX EAPOL Start	The number of EAPOL-Start frames received on the port.
RX EAPOL Logoff	The number of EAPOL-Logoff frames received on the port.
RX EAPOL Invalid	The number of invalid EAPOL frames received on the port.
RX EAPOL Total	The total number of EAPOL frames received on the port.
RX EAP Resp/Id	The number of EAP-Response/Identity frames received on the port
RX EAP Resp other than Resp/Id	The total number of EAPOL-Response frames received on the port that were not EAP-Response/Identity frames.
RX EAP Length Error	The number of EAPOL frames received on the port that have an invalid packet body length.
Last EAPOL Version	The version number of the last EAPOL frame received on the port.
Last EAPOL Source	The source MAC address in the last EAPOL frame received on the port.
TX EAPOL Total	The total number of EAPOL frames transmitted on the port.
TX EAP Req/Id	The number of EAP-Request/Identity frames transmitted on the port.
TX EAP Req other than Req/Id	The number of EAP-Request frames transmitted on the port that were not EAP-Request/Identity frames.

Examples The following example displays dot1x authentication statistics for port 10/2/1.

```
device# show dot1x statistics ethernet 10/2/1

Port 10/2/1 Statistics:
RX EAPOL Start : 2
RX EAPOL Logoff : 2
RX EAPOL Invalid : 0
RX EAPOL Total : 12
RX EAP Resp/Id : 4
RX EAP Resp other than Resp/Id : 4
RX EAP Length Error : 0
Last EAPOL Version : 1
Last EAPOL Source : 0022.0002.0002
TX EAPOL Total : 0
TX EAP Req/Id : 10417
TX EAP Req other than Req/Id : 2
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka config

Shows the MACsec Key Agreement (MKA) configuration for the device.

Syntax **show dot1x-mka config**

Modes EXEC or Privileged EXEC mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

Command Output The **show dot1x-mka config** command displays the following information:

Output field	Description
dot1x-mka-enable	MACsec is enabled on the device.
enable-mka ethernet *device/slot/port*	The ethernet interfaces specified are enabled for MACsec.
mka-cfg-group *group-name*	The configuration details that follow are for the named MACsec MKA group.
key-server-priority *value*	The key server priority for MACsec transmissions on the named group is set at this value.
macsec cipher-suite gcm-aes-128 or macsec cipher-suite gcm-aes-128 integrity-only	MACsec encryptions between members of the group are encrypted. or ICV checking only is performed, but no encryption is performed.
macsec confidentiality-offset *value*	The byte offset used for encrypted data is set to the value shown. Allowable values are 0, 30 (the first 30 bytes of data are not encrypted), and 50 (the first 50 bytes of data are not encrypted).
macsec frame-validation { check | discard }	For transmissions between MKA group members, indicates whether the MACsec frame header is checked and what action is taken for invalid frames (counted or discarded).
macsec-replay protection { strict | out-of-order window-size *value* }	Replay protection is enabled. The type of protection is shown as strict (discard any frame received out of sequence) or as allowing receipt of out-of-sequence frames within the specified window.
key *value* name *value*	The pre-shared key is set to this value and name for the MKA configuration group. Both key and name are hexadecimal strings.

Output field	Description
enable ethernet *device/slot/port* mka-cfg-group *name* key *hexadecimal value* name *hexadecimal value*	The specified interface is enabled for MACsec. The interface belongs to the named MKA group, and the interface uses the pre-shared key shown to confirm peers with which it can communicate.

Examples

The following example displays MACsec configuration information for an ICX 6610 device with MACsec enabled. Two MKA groups, test1 and group1, are configured. Interfaces with either group of parameters applied could form secure channels because the groups have the same pre-shared key.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka config

dot1x-mka-enable
 mka-cfg-group test1
  key-server-priority 5
  macsec cipher-suite gcm-aes-128 integrity-only
  macsec confidentiality-offset 30
  macsec frame-validation strict
mka-cfg-group group1
  key-server-priority 20
  macsec cipher-suite gcm-aes-128
  macsec confidentiality-offset 30
 enable-mka ethernet 1/3/2
  mka-group test1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d
fe347846 cce52c7d
 enable-mka ethernet 1/3/3
  mka-group group1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d
fe347846 cce52c7d
 enable-mka ethernet 1/3/4
  mka-group group1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d
fe347846 cce52c7d
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka config-group

Shows details for the specified MACsec Key Agreement (MKA) groups configured on this device, or for a designated MKA group.

Syntax **show dot1x-mka config-group** *group-name*

Parameters ***group-name***

Limits the group configuration displayed to the named MKA group.

Modes EXEC or Privileged EXEC mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

Command Output The **show dot1x-mka config-group** command displays the following information:

Output field	Description
mka-cfg-group	The configuration details that follow are for the specified MACsec MKA group.
key-server-priority	The key-server priority for MACsec transmissions on the named group is set at te specified value.
macsec cipher-suite gcm-aes-128 or macsec cipher-suite gcm-aes-128 integrity-only	MACsec transmissions are encrypted. or ICV checking only is performed.
macsec confidentiality-offset	The byte offset used for encrypted data is set to the value shown. Allowable values are 0, 30 (the first 30 bytes of data are not encrypted), and 50 (the first 50 bytes of data are not encrypted).
macsec frame-validation {check | discard}	Indicates whether the MACsec frame header is checked and what action is taken for invalid frames (counted or discarded).
macsec replay-protection {strict | out-of-order window-size *size*}	Replay protection is enabled. The type of protection is shown as strict (discard any frame received out of sequence) or as allowing receipt of out-of-sequence frames within the specified window.

Examples The following example lists the configuration details for MKA group test1.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka config-group test1

mka-cfg-group test1
  key-server-priority 5
  macsec cipher-suite gcm-aes-128 integrity-only
  macsec confidentiality-offset 30
  macsec frame-validation check
        macsec replay-protection strict
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka sessions

Displays a summary of all MACsec Key Agreement (MKA) sessions on the device.

Syntax **show dot1x-mka sessions brief**

show dot1x-mka sessions ethernet *device*/*slot*/*port*

Parameters **brief**

Displays a brief status of all MKA sessions.

ethernet ***device*/*slot*/*port***

Displays MKA sessions that are active on a specified Ethernet interface. The Ethernet interface is specified by device position in stack, slot on the device, and interface on the slot.

Modes EXEC or Privileged EXEC mode

Usage Guidelines This command is supported only on the Brocade ICX 6610.

Command Output The **show dot1x-mka sessions** command with the **brief** option displays the following information:

Output field	Description
Port	Designates the interface for which MACsec information is listed (by device, slot, and port).
Link-Status	Indicates whether the link is up or down.
MKA-Status	Indicates whether a secure channel has been established.
Key-Server	Indicates whether the interface is operating as a key-server.
Negotiated Capability	Indicates MACsec parameters configured on the designated interface.

The **show dot1x-mka sessions** command with the **ethernet** interface options displays the following information:

Output field	Description
Interface	The information that follows applies to the designated interface.
MKA cfg group Name	The designated MKA configuration group has been applied to the designated interface.
DOT1X-MKA Enabled (Yes, No)	Indicates whether MACsec is enabled for the designated interface.
DOT1X-MKA Active (Yes, No)	Indicates whether MACsec is active on the interface.
Key Server (Yes, No)	Indicates whether the MACsec key-server is active over the interface.
Configuration Status:	The following fields describe the MKA configuration applied to the interface.
Enabled (Yes, No)	Indicates whether MACsec is currently enabled.
Capability (Integrity and or confidentiality)	Indicates whether ICV checks are being performed on MACsec frames and whether encryption is being applied.

Output field	Description
Desired (Yes, No)	Indicates whether port is interested in becoming the key-server.
Protection (Yes, No)	Indicates whether replay protection is applied to the interface.
Frame Validation (Yes, No)	Indicates whether frames received are being checked for valid MACsec headers.
Replay Protection (Strict, Out of Order)	Indicates that replay protection is configured and whether frames must be received in exact order or within an allowable window.
Replay Protection Size	Indicates the allowable window size within which frames may be received.
Cipher Suite (GCM-AES-128)	Specifies the cipher suite used for ICV checking, encryption, and decryption.
Key Server Priority (1 to 127)	Specifies the key-server priority configured on the interface.
Secure Channel Information	The following fields describe a secure channel established on this interface.
Local SCI	Provides the hexadecimal value of the Secure Channel Identifier for this channel.
Member Identifier	Provides the MACsec number assigned to the MKA peer.
Message Number	Provides the Message Number contained in Hello packets from this MKA peer. Hello packets are exchanged to determine peer status, MACsec capabilities, and SAK Key Identifier.
Latest SAK Status (RX and or TX)	Indicates the Secure Association Key (SAK) state.
Latest SAK AN	Provides the Association Number for the most recently active Secure Association Key.
Latest SAK KI	Provides the Key Identifier for the most recently active Secure Association Key.
Negotiated Capability (Integrity and or Confidentiality with offset)	Indicates whether ICV checking, encryption, and a confidentiality offset have been applied on the secure channel. (The negotiated capability may differ from parameters configured on the interface when it does not have key-server status.)
Peer Information:	The output fields that follow provide information on actual and potential MACsec peer interfaces.
State (Live or Potential)	Indicates whether the peer is considered a live peer or a potential peer for MKA protocol.
Member Identifier	Designates the peer by its Member Identifier, a hexadecimal value.
Message Number	Provides the Message Number that appears in Hello packets from the designated peer interface as a hexadecimal value.
SCI	Provides the peer's Secure Channel Identifier.
Priority	Provides the key-server priority configured on the peer interface.

Examples

In the following example, all enabled MKA interfaces on the device are listed, along with configured parameters and current status.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka sessions brief

Port    Link-Status  MKA-Status  Key-Server  Negotiated Capability

1/3/2   Down         Pending     ---         ---
1/3/3   Up           Secured     No          Integrity, Confidentiality with Off. 30
1/3/4   Up           Secured     No          Integrity, Confidentiality with Off. 30
```

The following example lists MKA sessions that are active on Ethernet interface 1/3/3 (device 1, slot 3, port 3), with configuration details for each active interface.

```
device(config-dot1x-mka-1/3/3)# show dot1x-mka sessions ethernet 1/3/3

Interface                : 1/3/3

  MACsec Status          : Secured
  DOT1X-MKA Enabled      : Yes
  DOT1X-MKA Active       : Yes
  Key Server             : No

Configuration Status:
  Enabled                : Yes
  Capability             :  Integrity,  Confidentiality
  Desired                : Yes
  Protection             : Yes
  Frame Validation       : Disable
  Replay Protection      : Strict
  Replay Protection Size : 0
  Cipher Suite           : GCM-AES-128
  Key Server Priority    : 20

  Local SCI              : 748ef8344a510082
  Member Identifier      : 802ed0536fcafc43407ba222
  Message Number         : 8612

Secure Channel Information:
  Latest SAK Status      : Rx & Tx
  Latest SAK AN          : 0
  Latest KI              : d08483062aa9457e7c2470e300000001
  Negotiated Capability  : Integrity, Confidentiality with offset 30

Peer Information:
State        Member Identifier           Message Number    SCI
Priority
-----        -----------------           --------------    -----------------
--------
Live         d08483062aa9457e7c2470e3              8527    748ef83443910082
20
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka statistics

Displays current MACsec Key Agreement (MKA) statistics on the interface.

Syntax **show dot1x-mka statistics ethernet** *device*/*slot*/*port*

Parameters **ethernet** *device*/*slot*/*port*

Ethernet interface for which MKA statistics are to be displayed. The interface is designated by a device number in stack/slot on the device/interface on the slot.

Modes EXEC or Privileged EXEC mode

Usage Guidelines This command is supported only on the ICX 6610.

It is recommended that you use the **clear dot1x-mka statistics** command to clear results of the previous **show dot1x-mka statistics** command before re-executing it.

Command Output The **show dot1x-mka statistics** command displays the following information:

Output field	Description
Interface (device/slot/port)	The output fields describe MACsec activity for the designated interface.
MKA in Pkts	MKA protocol packets received
MKA in SAK Pkts	MKA protocol packets received containing a SAK
MKA in Bad Pkts	MKA protocol packets received that are bad
MKA in Bad ICV Pkts	MKA protocol packets received with a bad ICV
MKA in Mismatch Pkts	MKA protocol packets received with mismatched CAK
MKA out Pkts	MKA protocol packets transmitted
MKA out SAK Pkts	MKA protocol packets transmitted containing a SAK
Number of SAK	Total number of SAKs received

Examples The following example shows MKA statistics for Ethernet interface 1/3/3 (device 1, slot 3, port 3), which is transmitting and receiving MACsec frames.

```
device(config-dot1x-mka-1/3/3)# clear dot1x-mka statistics ethernet 1/3/3
device(config-dot1x-mka-1/3/3)# show dot1x-mka statistics ethernet 1/3/3

Interface                : 1/3/3

MKA in Pkts              : 8585
MKA in SAK Pkts          : 1
MKA in Bad Pkts          : 0
MKA in Bad ICV Pkts      : 0
MKA in Mismatch Pkts     : 0
MKA out Pkts             : 8687
MKA out SAK Pkts         : 0
Number of SAK            : 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show interface ethernet

Displays the detailed interface configuration and capabilities of all interfaces or for a specific interface.

Syntax **show interface ethernet** *stackid*/*slot*/*port*

Parameters *stackid*/*slot*/*port*

Specifies the Ethernet port.

Modes Privileged EXEC mode

Examples Thie following example shows detailed interface information. Note that the priority flow control (PFC) is shown as enabled and information for the unicast and multicast egress queues is shown separately.

```
Device#show interface ethernet 1/1/22

10GigabitEthernet1/1/22 is up, line protocol is up
  Port up for 16 minutes 1 seconds
  Hardware is 10GigabitEthernet, address is aabb.ccdd.ef14 (bia aabb.ccdd.ef14)
  Configured speed 10Gbit, actual 10Gbit, configured duplex fdx, actual fdx
  Member of 1 L2 VLANs, port is tagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0, mac-learning is enabled
  ….
  …..
  MTU 1500 bytes
  Priority-Flow-Control is Enabled
  300 second input rate: 37014512 bits/sec, 9036 packets/sec, 0.38% utilization
  300 second output rate: 731174584 bits/sec, 178509 packets/sec, 7.58% utilization
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  26055807 packets output, 13340529672 bytes, 0 underruns
  Transmitted 0 broadcasts, 98 multicasts, 26055709 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled

UC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                 0             2074860
         1           2349160             2074861
         2           2349163             2074861
         3           2349165             2074860
         4           2349163             2074860
         5           2349165             2074860
         6           5461694              518651
         7           6498353                   0


MC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                   0                   0
         1                   0                   0
         2                   0                   0
         3                   0                   0
         4                   0                   0
```

This example shows information for an interface that has an ingress profile and an egress profile attached to a port.

```
Device(config-if-e40000-1/1/1)#show inernet ethernet 1/1/1
40GigabitEthernet1/1/1 is up, line protocol is up
  Port up for 5 days 12 hours 45 minutes 48 seconds
  Hardware is 40GigabitEthernet, address is 748e.f8f9.3d80 (bia 748e.f8f9.3d80)
  Configured speed 40Gbit, actual 40Gbit, configured duplex fdx, actual fdx
  Configured mdi mode AUTO, actual none
  Member of 1 L2 VLANs, port is tagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0, mac-learning is enabled
  Flow Control is enabled
  Mirror disabled, Monitor disabled
  Mac-notification is disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  IPG MII 96 bits-time, IPG GMII 96 bits-time
  MTU 1500 bytes, encapsulation ethernet
  Ingress Profile is i1
  Egress Profile is e1
  300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  8060797794 packets input, 1031782117647 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 8060797794 unicasts
  4 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  8078157201 packets output, 1034004121728 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 8078157201 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled
```

History

Release version	Command history
8.0.20	This command was modified to include PFC status and separate unicast and multicast egress queues.

show interfaces stack-ports

Use the **show interfaces stack-ports** command to display information about the stacking ports for all members in a stack.

Syntax **show interfaces stack-ports**

Modes Privileged EXEC mode

Usage Guidelines Use the **clear stack ipc** command before issuing the**show stack ipc** command. This helps to ensure that the data are the most recent traffic statistics for the stack.

This command must be executed from active stack controller.

Command Output The **show interfaces stack-ports** command displays the following information:

Output field	Description
Port	Specifies the stack identification number for this unit
Link	Identifies the configuration for modules on this unit
State	Indicates that a priority has been assigned to this stack unit
Dupl	Indicates whether the port is configured as half- or full-duplex
Speed	Indicates the port speed
Trunk	Indicates whether the port is part of a trunk
Tag	Indicates whether the port is tagged or untagged
P	Specifies port priority
MAC	Provides the MAC address of the port. **NOTE** If a unit is provisional (it is reserved and does not have a physical unit associated with the unit ID), the interface MAC address displayed for the unit is 0000.0000.0000.
Name	Displays the optional name assigned to the port if present

Examples The following example displays information about the stack-port interfaces for an ICX 6610 in a mixed stack.

```
ICX6610-48 Router# show interfaces stack-ports
Port    Link    State   Dupl Speed Trunk Tag Pvid Pri MAC            Name
1/2/1   Up      Forward Full 40G   None  No  N/A  0   0000.0034.1db5
1/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.1db6
1/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.1db7
1/2/7   Down    None    None None  None  No  N/A  0   0000.0034.1db8
2/2/1   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/2   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/6   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/7   Down    None    None None  None  No  N/A  0   0000.0000.0000
3/2/1   Down    None    None None  None  No  N/A  0   0000.0034.266d
3/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.266e
3/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.266f
3/2/7   Up      Forward Full 10G   None  No  N/A  0   0000.0034.2670
5/2/1   Down    None    None None  None  No  N/A  0   0000.0034.11ad
5/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.11ae
5/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.11af
5/2/7   Down    None    None None  None  No  N/A  0   0000.0034.11b0
```

show ip mroute

Displays information on multicast routes. You can specify whether you want to display information from static or connected mroutes or from a particular mroute.

Syntax **show ip mroute** [**vrf** *vrf-name*] { **static** | **connected** | **nexthop** | *ip-subnet* [*mask*]}

Parameters

vrf *vrf-name*

Specifies a VRF route.

static

Specifies a static multicast route.

connected

Specifies a directly attached (connected) multicast route.

nexthop

Specifies an IPv4 next hop table.

ip-subnet [*mask*]

Specifies an IP address.

Modes Privileged EXEC mode

Global configuration mode

Examples The following example displays information for IP multicast routes:

```
Device(config)# show ip mroute

Total number of IP routes: 5
 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
       Destination             Gateway             Port             Cost
Type    Uptime
1       20.20.20.0/24           220.220.220.1       ve 220           1/1
S      8m54s
2       50.50.50.0/24           DIRECT              ve 50            0/0
D      8h26m
3       77.1.1.1/32             DIRECT              loopback 1       0/0
D      8h26m
4       129.129.129.0/24        DIRECT              ve 129           0/0
D      8h26m
5       220.220.220.0/24        DIRECT              ve 220           0/0
D      2h49m
```

The following example displays information for static multicast routes:

```
Device(config)# show ip mroute static

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
       Destination              Gateway          Port           Cost   Type   Uptime
1       20.20.20.0/24            220.220.220.1    ve 220         1/1    S      8m54s
```

The following example displays information for directly attached multicast routes:

```
Device(config)# show ip mroute connected

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
       Destination             Gateway           Port          Cost   Type   Uptime
1       50.50.50.0/24           DIRECT            ve 50         0/0    D      8h26m
2       77.1.1.1/32             DIRECT            loopback 1    0/0    D      8h26m
3       129.129.129.0/24        DIRECT            ve 129        0/0    D      8h26m
4       220.220.220.0/24        DIRECT            ve 220        0/0    D      2h49m
```

The following example displays information for IP multicast route 50.50.50.100:

```
Device(config)# show ip mroute 50.50.50.100

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
       Destination             Gateway           Port          Cost   Type   Uptime
1       50.50.50.0/24           DIRECT            ve 50         0/0    D      8h26m
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ip msdp mesh-group

Displays the details of a specific mesh-group.

Syntax **show ip msdp** [**vrf** *vrf-name*] **mesh-group** *group-name*

Parameters

vrf
: Displays the mesh-group details for the VRF instance specified by the *vrf-name* variable.

vrf-name
: Specifies the VRF instance.

mesh-group
: Specifies the MSDP group.

group-name
: Specifies the mesh group.

Modes Privileged EXEC mode

Global configuration mode

MSDP router configuration mode

Usage Guidelines If used without specifying a VRF, this command shows data from the default VRF.

Command Output The **show ip msdp** [**vrf** *vrf-name*] **mesh-group** *group-name* command displays the following information:

Output field	Description
Peer Address	The IP address of the MSDP peer that is placed in the mesh group.
State	The state of the MSDP device connection with the mesh group. The state can be one of the following: • CONNECT - The session is in the active open state. • ESTABLISH - The MSDP session is fully up. • IDLE - The session is idle. • LISTEN - The session is in the passive open state.
KA (Keep Alive) In	The number of MSDP keepalive messages received by the mesh group.
KA (Keep Alive) Out	The number of MSDP keepalive messages sent by the mesh group.
SA (Source-Active) In	The number of SA messages received by the mesh group.
SA (Source-Active) Out	The number of SA messages sent by the mesh group.
NOT (Notification) In	The number of notification messages received by the mesh group.
NOT (Notification) out	The number of notification messages sent by the mesh group.
Age	The number of seconds the messages has been in the cache.

Examples The following example shows the mesh-group configuration details.

```
device#show ip msdp mesh-group
Mesh-Group-Name                    Peer-IP-Address
group1                               40.0.0.40
group2                               21.0.0.23
```

The following example shows the details of mesh-group group1.

```
device#show ip msdp mesh-group group1
MSDP MESH-GROUP:group1
 KA: Keepalive SA:Source-Active NOT: Notification
 Peer Address    State          KA              SA             NOT         Age
                                In     Out    In     Out     In     Out
 40.0.0.40       ESTABLISH    1407    1406      0      0      0      0      6
```

The following example shows the mesh-group configuration details for the VRF 10 instance.

```
device#show ip msdp vrf 10 mesh-group
Mesh-Group-Name                    Peer-IP-Address
group1                               22.0.0.22
group2                               21.0.0.23
```

The following example shows the mesh-group group2 details for the VRF 10 instance.

```
device#show ip msdp vrf 10 mesh-group group2
MSDP MESH-GROUP:group2
KA: Keepalive SA:Source-Active NOT: Notification
Peer Address    State          KA           SA           NOT         Age
                                         In     Out   In     Out    In     Out
21.0.0.23           IDLE       0      0      0      0      0      0      0
```

History

Release version	Command history
08.0.20	This command was introduced.

show ip multicast group

Displays information about IGMP groups.

Syntax **show ip multicast** [**cluster**] **group** [*group-address* [**detail**] [**tracking**]]

Parameters

cluster
Specifies a multi-chassis trunking (MCT) cluster.

group-address
Specifies information for a particular group.

detail
Specifies detailed IGMP group information for a specific group.

tracking
Specifies tracking information on interfaces that have tracking enabled.

Modes Privileged EXEC mode

Command Output The **show ip multicast group** command displays the following information:

Output Field	Description
group	The address of the group (destination address in this case, 224.1.1.1)
p-port	The physical port on which the group membership was received.
ST	**Yes** indicates that the IGMP group was configured as a static group; **No** means the address was learned from reports.
QR	**Yes** means the port is a querier port; No means it is not. A port becomes a non-querier port when it receives a query from a source with a lower source IP address than the device.
life	The number of seconds the group can remain in EXCLUDE mode. An EXCLUDE mode changes to INCLUDE mode if it does not receive an "IS_EX" or "TO_EX" message during a certain period of time. The default is 260 seconds. There is no life displayed in INCLUDE mode.
mode	Indicates current mode of the interface: INCLUDE or EXCLUDE. If the interface is in INCLUDE mode, it admits traffic only from the source list. If an interface is in EXCLUDE mode, it denies traffic from the source list and accepts the rest.
source	Identifies the source list that will be included or excluded on the interface. For example, if an IGMP V2 group is in EXCLUDE mode with a source of 0, the group excludes traffic from the 0 (zero) source list, which actually means that all traffic sources are included.

Examples The following example shows that an IGMP V2 group is in EXCLUDE mode with a source of 0. The group excludes only traffic from the 0 (zero) source list, which means that all traffic sources are included.

```
Device#show ip multicast group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 3 groups, 4 group-port, tracking_enabled
      group           p-port   ST     QR     life mode    source
1     224.1.1.2       1/33     no     yes    120  EX      0
2     224.1.1.1       1/33     no     yes    120  EX      0
3     226.1.1.1       1/35     yes    yes    100  EX      0
4     226.1.1.1       1/33     yes    yes    100  EX      0
```

The following example displays detailed IGMP group information for multicast group 226.1.1.1:

```
Device#show ip multicast group 226.1.1.1 detail
Display group 226.1.1.1 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 2 group-port, tracking_enabled
      group           p-port   ST     QR     life mode    source
1     226.1.1.1       1/35     yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
      group           p-port   ST     QR     life mode    source
2     226.1.1.1       1/33     yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
```

The following example displays the list of clients that belong to multicast group 224.1.1.1 when tracking and fast leave are enabled:

```
Device#show ip multicast group 224.1.1.1 tracking
Display group 224.1.1.1 in all interfaces with tracking enabled.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 1 group-port, tracking_enabled
      group           p-port   ST     QR     life mode    source
*** Note: has 1 static groups to the entire vlan, not displayed here
1     224.1.1.1       1/33     no     yes    100  EX      0
    receive reports from 1 clients: (age)
      (10.2.100.2 60)
```

The following example displays information for a device in an MCT cluster, In the “local” column, YES indicates that report/leave were received on local ports [cluster-edge ports (CEP) or cluster-client-edge ports (CCEP)]; NO indicates that report/leave were received on a port that is an inter-chassis link (ICL) between the MCT cluster switches, via an MCT peer.

```
Device#show ip multicast cluster group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 1 group-port
      group           p-port   ST     QR     life  mode    source     local
1     225.1.1.1       e3/10    no     no     260   EX      0          YES
2     230.1.1.2       e3/12    no     yes    40    EX      0          NO
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.

show ip multicast mcache

Displays information in the multicast forwarding mcache.

Syntax **show ip multicast** [**cluster**] **mcache**

Parameters **cluster**

Specifies a multi-chassis trunking (MCT) cluster.

Modes Privileged EXEC mode

Usage Guidelines Configuring the **show default values** command does not show complete output; it shows only IGMP mcache values. The IGMP snooping mcache contains multicast forwarding information for VLANs and you must configure the **show ip multicast mcache** command to display those.

Command Output The **show ip multicast mcache** command displays the following information:

Field	Description
(source group)	Source and group addresses of this data stream. (* group) means match group only; (source group) means match both.
cnt	The number of packets processed in software. Packets are switched in hardware, which increases this number slowly.
OIF	The output interfaces. If `entire vlan` is displayed, this indicates that static groups apply to the entire VLAN.
age	The mcache age. The mcache will be reset to 0 if traffic continues to arrive, otherwise the mcache will be aged out when it reaches the time defined by the **ip multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	Vidx specifies output port list index. Range is from 4096 through 8191.
ref-cnt	The vidx is shared among mcaches having the same output interfaces. Ref-cnt indicates the number of mcaches using this vidx.
ICL	Inter-chassis link between MCT cluster switches.
CCEP	Cluster-client-edge ports (ports on cluster switch connecting it with acluster client).

Examples The following example shows information in the multicast forwarding mcache:

```
Device#show ip multicast mcache
Example: (S G) cnt=: cnt is number of SW processed packets
    OIF: e1/22 TR(1/32,1/33), TR is trunk, e1/32 primary, e1/33 output
vlan 10, 1 caches. use 1 VIDX
1    (10.10.10.2 239.0.0.3) cnt=0
     OIF: tag e2
     age=2s up-time=2s change=2s vidx=8191 (ref-cnt=1)
```

The following example shows information in the multicast forwarding mcache when data arrives locally:

```
Device#show ip multicast cluster mcache
xample: (S G) cnt=: (S G) are the lowest 32 bits, cnt is number of SW processed
packets
    OIF: e1/22 TR(e1/32,e1/33), TR is trunk, e1/32 primary, e1/33 output
         [1,10]: [1 - has local oif, 10 - ICL due to CCEP count]

vlan 10, 1 caches. use 1 VIDX
1    (* 225.1.1.3) cnt=52244
     OIF: tag TR(e4/23) [1,0]
     age=167s up-time=11548s, change=58639s vidx=8184 (ref-cnt=1)
```

The following example shows information in the multicast forwarding mcache when data arrives on an MCT peer:

```
Device#show ip multicast cluster mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt is number of SW processed
packets
    OIF: e1/22 TR(e1/32,e1/33), TR is trunk, e1/32 primary, e1/33 output
         [1,10]: [1 - has local oif, 10 - ICL due to CCEP count]

vlan 10, 1 caches. use 1 VIDX
1    (30.0.0.10 225.1.1.3) cnt=30084
     OIF: tag TR(e3/13) [1,0]
     age=152s up-time=13728s, change=9990s vidx=8184 (ref-cnt=1)
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.

show ip multicast optimization

Displays Internet Group Management Protocol (IGMP) snooping hardware resource-sharing information.

Syntax **show ip multicast optimization** [**ipmc**]

Parameters **ipmc**

Specifies the IPMC group index number.

Modes Privileged EXEC mode

VLAN configuration mode

Usage Guidelines The **show ip multicast optimization** command is available only on ICX 7750 devices.

Use this command to display the availability of IP multicast (IPMC) group indexes in the hardware and how they are used and shared.

Examples The following example displays resource information showing that IPMC group index 4 is shared by two users and the ports included in the set are 1/1/6 and 1/1/1:

```
Device(config)#vlan 150
Device(config-vlan-150)#show ip multicast optimization
Total IPMCs Allocated:    0; Available: 8192; Failed:    0
Index    IPMC         SetId          Users          Set
   1.    4             0x161fcbd8        2 {<1/1/6>,<1/1/1>,}
   2.    1             0x161d0930       10 {<1/1/6>,<1/1/4>,<1/1/3>,<1/1/2>,
                                           <1/1/1>,}
Sharability Coefficient:  76%
```

History

Release version	Command history
8.0.10	This command was introduced.

show ip multicast pimsm-snooping

Displays information related to PIM sparse mode (SM) snooping on the mcache.

Syntax **show ip multicast pimsm-snooping** [**vlan** *vlan-id*] [**cache** *ip-address*] [**resources**]

Parameters

cache *ip-address*

Specifies the PIM SM Snooping cache.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes Privileged EXEC mode

Usage Guidelines Use the **show ip multicast pimsm-snooping** command to display information related to the PIM SM snooping on the outgoing interface (OIF) in the mcache.

Examples The following example shows PIM SM information for the mcache:

```
Device#show ip multicast pimsm-snooping
Example: Port: 7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 225.1.1.1) has 3 pim join ports out of 4 OIF
     4/23 (ref_count=2), 4/13 (ref_count=1), 4/5 (ref_count=3),
```

show ip multicast vlan

Displays IGMP snooping information for a specific VLAN.

Syntax **show ip multicast vlan** [**cluster**] *vlan-id*

Parameters *vlan-id*

Specifies the VLAN for which you want information. If you do not specify a *vlan-id*, information for all VLANs is displayed.

cluster

Specifies a multi-chassis trunking (MCT) cluster.

Modes Privileged EXEC mode

Usage Guidelines You can use the **show ip multicast vlan** command to display the querier information for a VLAN. This command displays the VLAN interface status and whether there is any other querier present with the lowest IP address. The following list provides the combinations of querier possibilities:

- Active Interface with no other querier present
- Passive Interface with no other querier present
- Active Interface with other querier present
- Passive Interface with other querier present

Command Output The **show ip multicast vlan** command displays the following information:

Output Field	Description
Version	The global IGMP version. In this example, the device is configured for IGMP version 2.
Query	How often a querier sends a general query on the interface. In this example, the general queries are sent every 125 seconds.
Group Age	The number of seconds membership groups can be members of this group before aging out.
Max Resp	The maximum number of seconds a client waits before replying to a query.
Other Qr	How long it took a switch with a lower IP address to become a new querier. This value is 2 x Query + Max Resp.
cfg	The IGMP version for the specified VLAN. In this example, VL10: cfg V3 indicates that VLAN 10 is configured for IGMP V3.
vlan cfg	The IGMP configuration mode, which is either passive or active.
pimsm	Indicates that PIM SM is enabled on the VLAN.
rtr port	The router ports, which are the ports receiving queries.
local	Entries learned on local interfaces of the cluster switch, for example, local cluster-client-edge ports (CCEP) or cluster-edge ports (CEP).

Output Field	Description
mct peer	Entries learned via the MCT peer cluster switch. Control messages synchronize via inter-chassis link (ICL) from the MCT peer cluster switch.

Examples The following example shows IGMP snooping information for VLAN 10:

```
Device#show ip multicast vlan 10
Version=3, Intervals: Query=10, Group Age=260, Max Resp=10, Other Qr=30
VL10: cfg V3, vlan cfg passive, , pimsm (vlan cfg), 3 grp, 1 (SG) cache, no rtr port,
  e2      has    3 groups, non-QR (passive), default V3
  **** Warning! has V2 client (life=240),
    group: 239.0.0.3, life = 240
    group: 224.1.1.2, life = 240
    group: 224.1.1.1, life = 240
  e4      has    0 groups, non-QR (passive), default V3
```

The following example shows IGMP snooping information when the VLAN interface is active and no other querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft
 V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
  1/1/16  has    0 groups,
This interface is Querier
default V2
  1/1/24  has    0 groups,
This interface is Querier
default V2
  2/1/16  has    0 groups,
This interface is Querier
default V2
  2/1/24  has    0 groups,
This interface is Querier
default V2
  3/1/1   has    0 groups,
This interface is Querier
default V2
  3/1/4   has    0 groups,
This interface is Querier
default V2
```

The following example shows IGMP snooping information when the VLAN interface is passive and no other querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, no rtr port,
  1/1/16  has    0 groups,
This interface is non-Querier (passive)
default V2
  1/1/24  has    0 groups,
This interface is non-Querier (passive)
default V2
  2/1/16  has    0 groups,
This interface is non-Querier (passive)
default V2
  2/1/24  has    0 groups,
This interface is non-Querier (passive)
default V2
  3/1/1   has    0 groups,
This interface is non-Querier (passive)
default V2
  3/1/4   has    0 groups,
This interface is non-Querier (passive)
default V2
```

The following example shows IGMP snooping information when the VLAN interface is active and another querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg active, 7 grp, 6 (*G) cache, rtr ports,
    router ports: 2/1/24(260) 10.5.5.5, 3/1/4(260) 10.8.8.8,
  1/1/16  has    4 groups,
This interface is Querier
default V2
    group: 226.6.6.6, life = 240
    group: 228.8.8.8, life = 240
    group: 230.0.0.0, life = 240
    group: 224.4.4.4, life = 240
  1/1/24  has    1 groups,
This interface is Querier
default V2
    group: 228.8.8.8, life = 240
  2/1/16  has    4 groups,
This interface is Querier
default V2
    group: 226.6.6.6, life = 240
    group: 228.8.8.8, life = 240
    group: 230.0.0.0, life = 240
    group: 224.4.4.4, life = 240
  2/1/24  has    2 groups,
This interface is non-Querier
Querier is 10.5.5.5
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 234.4.4.4, life = 260
    group: 226.6.6.6, life = 260
  3/1/1   has    4 groups,
This interface is Querier
default V2
    group: 238.8.8.8, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  3/1/4   has    1 groups,
This interface is non-Querier
Querier is 10.8.8.8
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 236.6.6.6, life = 260
```

The following example shows IGMP snooping information when the VLAN interface is passive and another querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg passive, 7 grp, 6 (*G) cache, rtr ports,
    router ports: 2/1/24(260) 10.5.5.5, 3/1/4(260) 10.8.8.8,
  1/1/16  has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 226.6.6.6, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  1/1/24  has    1 groups,
This interface is non-Querier (passive)
default V2
    group: 228.8.8.8, life = 260
  2/1/16  has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 226.6.6.6, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  2/1/24  has    2 groups,
This interface is non-Querier (passive)
Querier is 10.5.5.5
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 234.4.4.4, life = 260
    group: 226.6.6.6, life = 260
  3/1/1   has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 238.8.8.8, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  3/1/4   has    1 groups,
This interface is non-Querier (passive)
Querier is 10.8.8.8
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 236.6.6.6, life = 260
```

The following example shows IGMP snooping information when the device is connected to an MCT cluster:

```
Device#show ip multicast cluster vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255

VL10: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, rtr ports,
    router ports: e4/14(65) 50.0.0.1 (local:1, mct peer:0)

(local:1, mct peer:0)     <- Indicates if entry is local or\and mct-peer entry
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.

show ip pim interface

Displays information for PIM interfaces.

Syntax **show ip pim interface** { **ethernet***stackid*/*slot*/*port-id* | **loopback** *loopback-number* | **ve** *ve-number* }

Parameters

ethernet*stackid*/*slot*/*port-id*

Specifies a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *loopback-number*

Specifies a loopback interface.

ve *ve-number*

Specifies a virtual interface.

Modes Privileged EXEC mode

Examples This example displays output from the **show ip pim interface** command, showing that ACL 10 is applied to interface 1/1/9 to control neighbor access.

```
Device# show ip pim interface
Flags    : SM  - Sparse Mode v2, DM - Dense Mode v2, P - Passive Mode

--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+

Int'face|Local          |Mode |St |Des Rtr|TTL|Mcast| Filter| VRF   |DR  |Override
        |Address        |     |   |AddPort|Thr|Bndry|  ACL  |       |Prio|Interval
--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+
e1/1/1   5.5.5.5         SM   Ena  Itself   1  None   None   default  1   3000ms
e1/1/9   15.1.1.5        SM   Ena  Itself   1  None   10     default  1   3000ms
e1/1/12  12.12.12.1      SM   Dis  Itself   1  None   None   default  1   3000ms
v20      21.21.21.22     SM   Ena  Itself   1  None   None   default  1   3000ms
v60      60.60.60.1      SM   Ena  Itself   1  None   None   default  1   3000ms
v310     110.110.110.2   SM   Dis  Itself   1  None   None   default  1   3000ms
v360     160.160.160.1   SM   Dis  Itself   1  None   None   default  1   3000ms
l2       4.4.4.4         SM   Ena  Itself   1  None   None   default  1   3000ms
l3       10.10.10.10     SM   Ena  Itself   1  None   None   default  1   3000ms
Total Number of Interfaces : 9
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show ip pim traffic

Displays IPv4 PIM traffic statistics.

Syntax **show ip pim traffic** [**vrf** *vrf-name*] [**join-prune**] [**rx** | **tx**]

Parameters

vrf *vrf-name*
Specifies information for a VRF instance.

join-prune
Specifies displaying join and prune statistics.

rx
Specifies displaying received PIM traffic statistics.

tx
Specifies displaying transmitted PIM traffic statistics.

Modes Privileged EXEC mode

Usage Guidelines PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. **NOTE** Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.

Examples This example shows PIM join and prune traffic statistics for received and sent packets:

```
Device(config)#show ip pim traffic
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     0         0           0         0         0         0         0         0
v50     2526      1260        0         0         0         1263      0         0
v150    2531      0           0         0         0         1263      0         0
v200    2531      0           0         0         0         1         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     2528      0           0         0         0         0         0
v50     2540      1263        0         0         0         2         0
v150    2529      0           0         0         0         1262      0
v200    2529      0           0         0         0         1262      0
```

This example shows the number of received IPv4 PIM Hello packets dropped on interface 1/1/9 because an ACL to control neighbor access is configured on it.

```
Device#show ip pim traffic rx
Port    HLO   JN-PRNE  ASSERT REG      REG       BTSTRP    CAND RP   Err
                              GRFT(DM) STOP(SM)  MSGS(SM)  ADV.(SM)

-------+-------+------+-----+-------+---------+---------+---------+---
        Rx      Rx     Rx    Rx      Rx         Rx        Rx        Rx
-------+-------+------+-----+-------+---------+---------+---------+---
e1/1/1  0       0      0     0       0          0         0         0
e1/1/9  764     0      0     0       0          0         0         757
e1/1/12 0       0      0     0       0          0         0         0
v20     758     0      0     1916    0          0         0         0
v60     0       0      0     0       0          0         0         0
v310    0       0      0     0       0          0         0         0
v360    0       0      0     0       0          0         0         0
```

This example shows PIM join and prune traffic statistics for sent packets:

```
Device(config)#show ip pim traffic tx
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     2528      0           0         0         0         0         0
v50     2540      1263        0         0         0         2         0
v150    2529      0           0         0         0         1262      0
v200    2530      0           0         0         0         1262      0
```

This example shows PIM join and prune traffic statistics.

```
Device(config)#show ip pim traffic join-prune
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Rx        Rx        Rx        Rx        Rx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1260      1260      0         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Tx        Tx        Tx        Tx        Tx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1263      1262      1         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

This example shows PIM join and prune traffic statistics.

```
Device(config)#show ip pim traffic join-prune rx
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Rx        Rx        Rx        Rx        Rx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1260      1260      0         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

This example shows PIM join and prune traffic statistics.

```
Device(config)#show ip pim traffic join-prune tx
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Tx        Tx        Tx        Tx        Tx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1264      1263      1         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

History

Release version	Command history
8.0.20a	This command was modified to display, in the Err column, received Hello packets dropped on an interface because of an ACL to control neighbor access.

show ip pimsm-snooping cache

Displays the downstream PIM join/prune information for both source-path tree (SPT) and rendezvous-point tree (RPT).

Syntax **show ip pimsm-snooping cache** [**vlan** *vlan-id*] *ip-address* [**resources**]

Parameters *ip-address*

Specifies the IP address.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes Privileged EXEC mode

Usage Guidelines Use the **show ip pimsm-snooping cache** command to check and verify the outgoing interfaces (OIF)s added by pimsm-snooping module.

Command Output The **show ip pimsm-snooping cache** command displays the following information:

Output field	Description
SG	(s,g) downstream fsm state for SPT.
G	(*,g) downstream fsm state for RPT

The **show ip pimsm-snooping cache** command displays the following information only when multi-chassis trunking (MCT) is enabled on the VLAN:

Output field	Description
CCEP	Cluster client edge port
CEP	Cluster edge port
Remote/Local	Join/Prune received on MCT peer or local

Examples The following example shows PIM SM information when there is no traffic and the last-hop router (LHR) has joined the RPT. Only an (*,G) entry is created.

```
Device1#show ip pimsm-snooping cache
 OIF Info:
 TR - OIF Belongs to Trunk/LAG, Primary port is displayed
 SG - (*,g)/(s,g) downstream fsm state:
      NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
 RPT - (s,g,rpt) downstream fsm state:
      NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
      join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
      in progress.

PIMSM Snoop cache for vlan 503
1     (* 225.1.1.1) Up Time: 5d 18:38:32
     OIFs: 2
     TR(e4/5) G : J(197) ET: 210, Up Time: 5d 18:38:32 , CCEP, Remote
     TR(e4/23) G : J(166) ET: 210, Up Time: 1d 19:36:23 , CEP, Local
```

The following example shows PIM SM information when there is traffic from source 30.0.0.10. An (S,G) entry is created and the LHR has joined the SPT.

```
Device2#show ip pimsm-snooping cache
  OIF Info:
 TR - OIF Belongs to Trunk/LAG, Primary port is displayed
 SG - (*,g)/(s,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
 RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

1    (* 225.1.1.1) Up Time: 5d 18:44:28
    OIFs: 2
    TR(e4/5) G : J(195) ET: 210, Up Time: 5d 18:44:28 , CCEP, Remote
    TR(e4/23) G : J(170) ET: 210, Up Time: 1d 19:42:18 , CEP, Local

2    (30.0.0.10 225.1.1.1) Up Time: 00:00:58
    OIFs: 2
    TR(e4/5) SG : J(202) ET: 210, Up Time: 00:00:58 , CCEP, Remote
    TR(e4/23) SG : J(168) ET: 210, Up Time: 00:00:58 , CEP, Local
```

The following example shows PIM SM resource information.

```
Device#show ip pimsm-snooping resources
                     alloc in-use  avail get-fail    limit  get-mem  size init
pimsm group entry     1000     10    990        0   232000       10    61 1000
pimsm source entry    2000     20   1980        0   464000       40    65 2000
pimsm oif entry       2000     30   1970        0   464000       59    89 2000

Total memory in used: 369000 bytes
```

show ip ssl

Displays SSL connection details.

Syntax **show ip ssl certificate**

Parameters **certificate**

Displays the SSL certificate details.

Modes Privileged EXEC mode

Global configuration mode

Examples The following example displays the output of the **show ip ssl** command.

```
device(config)#show ip ssl
Session Protocol Source IP      Source Port  Remote IP      Remote Port
1       TLS_1_2  10.20.157.102  634          10.25.105.201  60892
```

The following example displays the SSL certificate details.

```
device(config)#show ip ssl certificate
Trusted Certificates:
 Dynamic:
 Index 0:
  Signature Algorithm: sha256WithRSAEncryption
  Issuer:
   CN: 10.25.105.201
  Validity:
   Not Before: 2014 Aug 22 05:12:45
   Not After : 2017 Aug 21 05:12:45
  Subject:
   CN: 10.25.105.201
  X509v3 extensions:
   X509v3 Subject Alternative Name:
    IP Address: 10.25.105.201
  Signature:
   12:ec:41:d8:01:45:61:ce:cf:7e:80:de:a6:7c:a7:2e:01:7f:
   42:27:22:1d:ac:a2:47:c5:0d:4f:e3:68:24:de:bf:50:40:65:
   25:8c:30:bd:ff:a7:d0:21:73:d2:ba:5e:67:42:1f:bb:97:4a:
   d9:1d:c3:ca:31:c4:59:10:79:d1:42:f4:b6:1a:b0:98:4e:a8:
   ef:e2:a2:98:c3:14:16:63:50:02:a0:18:9c:7a:e3:17:39:0d:
   b7:30:ab:23:9f:63:bd:0f:9e:d8:67:b0:fe:ec:3b:fa:4c:f4:
   3d:34:e2:99:0e:99:24:ec:93:fb:8a:e5:4a:bf:74:d6:ff:91:
   0a:dc:fb:b9:4f:91:5d:d4:f6:77:23:eb:ec:eb:3a:62:08:e1:
   a6:ea:a8:52:b6:39:62:db:29:fa:61:1d:fd:d5:02:31:04:73:
   50:ad:de:41:54:a5:e2:96:2d:9c:f4:68:b2:68:05:bb:39:47:
   ee:74:89:a2:8c:30:f0:f9:d7:d5:4b:3b:e2:95:6f:82:61:a3:
   c2:79:4c:f2:11:56:f8:2f:cc:fc:2b:4b:cb:3b:54:59:f0:8b:
   5b:70:e1:27:c3:57:25:eb:35:c6:07:ea:6d:0b:34:04:95:81:
   35:e6:64:c6:b8:72:e8:24:18:bd:ca:90:99:74:45:44:85:71:
   9e:7f:13:96:
```

show ip static mroute

Displays information for configured multicast routes.

Syntax **show ip static mroute** [**vrf** *vrf-name*] *ip-subnet mask*]

Parameters **vrf** *vrf-name*

Specifies an optional VRF route.

ip-subnet mask

Specifies an IP address and an optional address mask.

Modes Privileged EXEC mode

Usage Guidelines Only resolved and best static mroutes are added to the mRTM table. These routes are prefixed with an asterisk in the output from the **show ip static mroute** command.

Examples The following example displays information for configured multicast routes:

```
Device(config)# show ip static mroute
IP Static Routing Table - 2 entries:
 IP Prefix          Next Hop        Interface  Dis/Metric/Tag  Name
*20.20.20.0/24      220.220.220.1   -          1/1/0
20.20.20.0/24       50.50.50.2      -          1/2/0
21.21.21.0/24       1.2.3.4         -          1/1/0
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ipv6 mroute

Displays information on IPv6 multicast routes. You can specify displaying information either from static or connected mroutes or from a particular mroute.

Syntax **show ipv6 mroute** [**vrf** *vrf-name*] { *ipv6-address ipv6-prefix/prefix-length* | **static** | **connect** | **summary** }

Parameters

vrf *vrf-name*

Specifies displaying mroutes for a particular VRF.

ipv6-address ipv6-prefix/prefix-length

Displays an IPv6 mroute for the specified destination.

static

Displays only static multicast routes.

connect

Displays only connected multicast routes.

summary

Displays summary information.

Modes Privileged EXEC mode

Examples The following example displays information for IPv6 multicast routes:

```
Device(config)# show ipv6 mroute
IPv6 Routing Table - 7 entries:
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
S    1:1::1:0/120          ::                 ve 90         1/1            2d16h
C    2090::/64             ::                 ve 90         0/0            6d21h
C    2100::/64             ::                 ve 100        0/0            1d21h
C    2110::/64             ::                 ve 110        0/0            1d21h
C    2120::/64             ::                 ve 120        0/0            1d21h
C    2130::/64             ::                 ve 130        0/0            6d21h
C    8811::1/128           ::                 loopback 1    0/0            6d21h
```

The following example displays information for static IPv6 multicast routes:

```
Device(config)# show ipv6 mroute static
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
S    1:1::1:0/120          ::                 ve 90         1/1            2d16h
```

The following example displays information for directly attached (connected) IPv6 multicast routes:

```
Device(config)#show ipv6 mroute connect
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
C    2090::/64             ::                 ve 90         0/0            6d21h
C    2100::/64             ::                 ve 100        0/0            1d21h
C    2110::/64             ::                 ve 110        0/0            1d21h
C    2120::/64             ::                 ve 120        0/0            1d21h
C    2130::/64             ::                 ve 130        0/0            6d21h
C    8811::1/128           ::                 loopback 1    0/0            6d21h
```

The following example displays information for IPv6 multicast route 2090::1:

```
Device(config)# show ipv6 mroute 2090::1
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
C    2090::/64             ::                 ve 90         0/0            6d21h
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ipv6 multicast mcache

Displays information in the IPv6 multicast forwarding mcache (multicast listening discovery [MLD]).

Syntax **show ipv6 multicast mcache**

Modes Privileged EXEC mode

Command Output The **show ipv6 multicast mcache** command displays the following information:

Output Field	Description
(abcd:ef50 0:100):	The lowest 32 bits of source and group. It is displayed in XXXX:XXXX hex format. Here XXXX is a 16-bit hex number.
cnt	The number of packets processed in software.
OIF	Output interfaces.
age	The mcache age in seconds. The mcache is reset to 0 if traffic continues to arrive, otherwise it is aged out when it reaches the time defined by the **ipv6 multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	The vidx is shared among mcaches using the same output interfaces. The vidx specifies the output port list, which shows the index. Valid range is from 4096 to 8191.
ref-cnt	The number of mcaches using this vidx.

Examples This example shows information in the multicast forwarding mcache:

```
Device#show ipv6 multicast mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt: SW proc. count
    OIF: 1/22 TR(1/32,1/33), TR is trunk, 1/32 primary, 1/33 output
vlan 1, has 2 cache
1    (abcd:ef50 0:100), cnt=121
     OIF: 1/11 1/9
     age=0s up-time=120s vidx=4130 (ref-cnt=1)
2    (abcd:ef50 0:101), cnt=0
     OIF: entire vlan
     age=0s up-time=0s vidx=8191 (ref-cnt=1)
vlan 70, has 0 cache
```

show ipv6 multicast group

Displays information about multicast listening discovery (MLD) groups.

Syntax **show ipv6 multicast group** [*group-address* [**detail**] [**tracking**]]

Parameters *group-address*

Specifies information for a particular group.

detail

Specifies the source list of a specific VLAN.

tracking

Specifies tracking information on interfaces that have tracking enabled.

Modes Privileged EXEC mode

Command Output The **show ipv6 multicast group** command displays the following information:

Output Field	Description
group	The address of the IPv6 group (destination IPv6 address).
p-port	The physical port on which the group membership was received.
ST	**Yes** indicates that the MLD group was configured as a static group; **No** means it was learned from reports.
QR	**Yes** means the port is a querier port; **No** means it is not. A port becomes a non-querier port when it receives a query from a source with a lower source IP address than the port.
life	The number of seconds the group can remain in EXCLUDE mode. An EXCLUDE mode changes to INCLUDE if it does not receive an IS_EX or TO_EX message during a specified period of time. The default is 140 seconds. There is no `life` displayed in INCLUDE mode.
mode	The current mode of the interface: INCLUDE or EXCLUDE. If the interface is in INCLUDE mode, it admits traffic only from the source list. If the interface is in EXCLUDE mode, it denies traffic from the source list and accepts the rest.
source	Identifies the source list that will be included or excluded on the interface. An MLDv1 group is in EXCLUDE mode with a source of 0. The group excludes traffic from 0 (zero) source list, which actually means that all traffic sources are included.
group	If you requested a *detailed* report, the following information is displayed: • The multicast group address • The mode of the group • Sources from which traffic will be admitted (INCLUDE) or denied (EXCLUDE) on the interface. • The life of each source list. If you requested a *tracking/fast leave* report, the clients from which reports were received are identified.

Examples This example shows that an MLDv1 group is in EXCLUDE mode with a source of 0. The group excludes only traffic from the 0 (zero) source list, which means that all traffic sources are included.

```
Device#show ipv6 multicast group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 263 grp, 263 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a0e3                       1/7    N  Y  120  EX   0
2     ff01::1:f123:f567                     1/9    N  Y       IN   1
```

This example displays detailed MLD group information for multicast group ff0e::ef00:a096:

```
Device#show ipv6 multicast group ff0e::ef00:a096 detail
Display group ff0e::ef00:a096 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a096                       1/7    N  Y  100  EX   0
    group: ff0e::ef00:a096, EX, permit 0 (source, life):
      life=100, deny 0:
```

This example displays the list of clients that belong to multicast group ff0e::ef00:a096 when tracking and fast leave are enabled:

```
Device#show ipv6 multicast group ff0e::ef00:a096 tracking
Display group ff0e::ef00:a096 in all interfaces with tracking enabled.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a096                       1/7    N  Y  80   EX   0
    receive reports from 1 clients: (age)
      (2001:DB8::1011:1213:1415 60)
```

show ipv6 multicast mcache

Displays information in the IPv6 multicast forwarding mcache (multicast listening discovery [MLD]).

Syntax **show ipv6 multicast mcache**

Modes Privileged EXEC mode

Command Output The **show ipv6 multicast mcache** command displays the following information:

Output Field	Description
(abcd:ef50 0:100):	The lowest 32 bits of source and group. It is displayed in XXXX:XXXX hex format. Here XXXX is a 16-bit hex number.
cnt	The number of packets processed in software.
OIF	Output interfaces.
age	The mcache age in seconds. The mcache is reset to 0 if traffic continues to arrive, otherwise it is aged out when it reaches the time defined by the **ipv6 multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	The vidx is shared among mcaches using the same output interfaces. The vidx specifies the output port list, which shows the index. Valid range is from 4096 to 8191.
ref-cnt	The number of mcaches using this vidx.

Examples This example shows information in the multicast forwarding mcache:

```
Device#show ipv6 multicast mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt: SW proc. count
    OIF: 1/22 TR(1/32,1/33), TR is trunk, 1/32 primary, 1/33 output
vlan 1, has 2 cache
1    (abcd:ef50 0:100), cnt=121
     OIF: 1/11 1/9
     age=0s up-time=120s vidx=4130 (ref-cnt=1)
2    (abcd:ef50 0:101), cnt=0
     OIF: entire vlan
     age=0s up-time=0s vidx=8191 (ref-cnt=1)
vlan 70, has 0 cache
```

show ipv6 multicast optimization

Displays multicast listening discovery (MLD) snooping hardware resource-sharing information.

Syntax **show ipv6 multicast optimization** [**l2mc**]

Parameters **l2mc**

Specifies the L2MC group index.

Modes Privileged EXEC mode

VLAN configuration mode

Usage Guidelines The **show ipv6 multicast optimization** command is supported only on ICX 7750 devices.

Use this command to display the availability of Layer 2 multicast (L2MC) group indexes in the hardware and how it is used and shared

Examples The following example displays resource information showing that L2MC group index 4 is shared by two users and the ports included in the set are 1/1/6 and 1/1/1:

```
Device (config)# vlan 150
Device (config-vlan-150)# show ipv6 multicast optimization
Total L2MCs Allocated:    0; Available: 8192; Failed:    0
Index    L2MC         SetId         Users         Set
   1.    4             0x161fcbd8        2 {<1/1/6>,<1/1/1>,}
   2.    1             0x161d0930       10 {<1/1/6>,<1/1/4>,<1/1/3>,<1/1/2>,
                                           <1/1/1>,}
Sharability Coefficient:  76%
```

History

Release version	Command history
8.0.10	This command was introduced.

show ipv6 multicast pimsm-snooping

Displays information related to PIM sparse mode (SM) snooping on the mcache.

Syntax **show ipv6 multicast pimsm-snooping** [**vlan** *vlan-id*] [**cache** *ipv6-address*] [**resources**]

Parameters

cache *ipv6-address*

Specifies the PIM SM Snooping cache.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes Privileged exec mode

Usage Guidelines Use the **show ipv6 pimsm-snooping cache** command to display information related to the PIM SM snooping outgoing interface (OIF) in the mcache.

Examples The following example shows PIM SM information for the mcache:

```
Device#show ipv6 multicast pimsm-snooping
Example: Port: 7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 2:3) has 1 pim join ports out of 1 OIF
     1/1/4 (ref_count=2),
```

show ipv6 multicast vlan

Displays display multicast listening discovery (MLD) snooping information for all VLANs or for a specific VLAN.

Syntax **show ipv6 multicast vlan** *vlan-id*

Parameters *vlan-id*

Specifies the VLAN for which you want information. If you do not specify a *vlan-id*, information for all VLANs is displayed.

Modes Privileged EXEC mode

Command Output The **show ipv6 multicast vlan** command displays the following information:

Output Field	Description
version	The MLD version number.
query-t	How often a querier sends a general query on the interface.
group-aging-t	Number of seconds membership groups can be members of this group before aging out.
rtr-port	The router ports which are the ports receiving queries. The display `router ports: 1/36(120) 2001:DB8::2e0:52ff:fe00:9900` means port 1/36 has a querier with 2001:DB8::2e0:52ff:fe00:9900 as the link-local address, and the remaining life is 120 seconds.
max-resp-t	The maximum number of seconds a client can wait before it replies to the query.
non-QR	Indicates that the port is a non-querier.
QR	Indicates that the port is a querier.

Examples This example shows MLD snooping information for VLAN 70:

```
Device#show ipv6 multicast vlan 70
version=1, query-t=60, group-aging-t=140, max-resp-t=3, other-qr-present-t=123
VL70: cfg V2, vlan cfg passive, 2 grp, 0 (SG) cache, rtr ports,
    router ports: 1/36(120) 2001:DB8::2e0:52ff:fe00:9900,
  1/26 has 2 grp, non-QR (passive), cfg V1
  1/26 has 2 grp, non-QR (passive), cfg V1
    group: ff10:1234::5679, life = 100
    group: ff10:1234::5678, life = 100
  1/35 has 0 grp, non-QR (QR=2001:DB8::2e0:52ff:fe00:9900, age=20), dft V2 trunk
```

show ipv6 neighbor

Displays the status of the neighbor discovery (ND) inspection configuration, details of the VLANs on which ND inspection is enabled, ND static entries, and ND inspection statistics.

Syntax **show ipv6 neighbor** [**vrf** *vrf-name*] **inspection** [**static-entry** | **statistics** | **vlan** *vlan-number*]

Parameters

static-entry

Specifies the manually configured static ND inspection entries that are used to validate the packets received on untrusted ports.

statistics

Specifies the total number of neighbor discovery messages received and the number of packets discarded after ND inspection.

vlan

Specifies the VLANs on which ND inspection is enabled.

vlan-number

Specifies the ID of the configured VLAN.

vrf

Specifies the VRF instance.

vrf-name

Specifies the ID of the VRF instance.

inspection

Specifies that the neighbor discovery messages are verified against the static ND inspection entries or dynamically learned DHCPv6 snoop entries.

Modes Privileged EXEC mode

Global configuration mode

VRF configuration mode

Command Output The **show ipv6 neighbor** command displays the following information.

Output field	Description
VLAN	The list of VLANs on which ND inspection is enabled.
IPv6 Address	The IPv6 addresses of the hosts that are added as static ND inspection entries.
LinkLayer-Addr	The MAC addresses of the hosts that are added as static ND inspection entries.
Total number of ND Solicit received	The total number of neighbor solicitation messages received.
Total number of ND Advert received	The total number of neighbor advertisement messages received.
Total number of Router Solicit received	The total number of router solicitation messages received.
Total number of ND dropped	The total number of neighbor discovery messages that are discarded because of the IP-to-MAC address binding discrepancy.
IPv6 Neighbor inspection VLAN *vlan-number*	The status of ND inspection on a VLAN.

Output field	Description
Untrusted Ports	The interfaces or member ports on which trust mode is not enabled.
Trusted Ports	The interfaces or member ports on which trust mode is enabled.

Examples The following example shows the output of the **show ipv6 neighbor inspection** command.

```
device(config)# show ipv6 neighbor inspection
IPv6 Neighbor inspection enabled on 2 VLAN(s):
        VLAN: 2
        VLAN: 3
```

The following example shows the output of the ND inspection configuration details for a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection
IPv6 Neighbor inspection enabled on 2 VLAN(s):
        VLAN: 2
        VLAN: 3
```

The following example shows the output of the **show ipv6 neighbor inspection static-entry** command.

```
device(config)# show ipv6 neighbor inspection static-entry
 Total number of ND Inspect entries: 3
 IPv6 Address                           LinkLayer-Addr
 2001::1                                0000.0000.1234
 2001::3                                0000.1234.4567
 2001::2                                0000.0000.4567
```

The following example shows the ND static entries of a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection static-entry
 Total number of ND Inspect entries: 1
 IPv6 Address                           LinkLayer-Addr
 2001:201:1:1::34                        cc4e.246d.2038
```

The following example shows the output of the **show ipv6 neighbor inspection statistics** command.

```
device(config)# show ipv6 neighbor inspection statistics
Total number of ND Solicit received      11
Total number of ND Advert received      29
Total number of Router Solicit received  20
Total number of ND dropped               6
```

The following example shows the ND inspection statistics of a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection statistics
Total number of ND Solicit received      11
Total number of ND Advert received      29
Total number of Router Solicit received  20
Total number of ND dropped               6
```

The following example shows the output of the **show ipv6 neighbor inspection vlan** *vlan-number* command.

```
device (config)# show ipv6 neighbor inspection vlan 2
IPv6 Neighbor inspection VLAN 2: Enabled
  Untrusted Ports : ethe 1/1/1 to 1/1/2
  Trusted Ports : ethe 1/1/3
```

The following example shows the details of the VLANs on which ND inspection is enabled for a VRF.

```
device (config-vrf-3)# show ipv6 neighbor vrf 3 inspection vlan 2
IPv6 Neighbor inspection VLAN 2: Enabled
  Untrusted Ports : ethe 1/1/1 to 1/1/2
  Trusted Ports : ethe 1/1/3
```

History

Release version	Command history
08.0.20	This command was introduced.

show ipv6 pim interface

Displays information for IPv6 PIM interfaces.

Syntax **show ipv6 pim interface** { **ethernet***stackid*/*slot*/*port-id* | **loopback** *loopback-number* | **ve** *ve-number* }

Parameters **ethernet***stackid*/*slot*/*port-id*

Specifies a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *loopback-number*

Specifies a loopback interface.

ve *ve-number*

Specifies a virtual interface.

Modes Privileged EXEC mode

Examples The following example displays output from the **show ipv6 pim interface** command, showing that ACL f10 is applied to interface 1/1/9 to control neighbor access.

```
Device# show ipv6 pim interface
Flags     : SM  - Sparse Mode v2

--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+

Int'face|Local          |Mode |St |Des Rtr|TTL|Mcast| Filter| VRF   |DR  |Override
        |Address        |     |   |Add Prt|Thr|Bndry|  ACL  |       |Prio|Interval
--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+
e1/1/1   3000::2         SM   Ena  Itself   1  None   None   default  1   3000ms
e1/1/9   201::1          SM   Ena  Itself   1  None   f10    default  1   3000ms
e1/1/12  1222::1         SM   Dis  Itself   1  None   None   default  1   3000ms
v20      2000::2         SM   Ena  Itself   1  None   None   default  1   3000ms
v60      6000::1         SM   Ena  Itself   1  None   None   default  1   3000ms
v310     1100::2         SM   Dis  Itself   1  None   None   default  1   3000ms
v360     1600::1         SM   Dis  Itself   1  None   None   default  1   3000ms
l2       4444::2         SM   Ena  Itself   1  None   None   default  1   3000ms
l3       7711::11        SM   Ena  Itself   1  None   None   default  1   3000ms
Total Number of Interfaces : 9
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show ipv6 pim traffic

Displays IPv6 PIM traffic statistics.

Syntax **show ipv6 pim traffic** [**vrf** *vrf-name*] [**join-prune**] [**rx** | **tx**]

Parameters

vrf *vrf-name*
Specifies information for a VRF instance.

join-prune
Specifies displaying join and prune statistics.

rx
Specifies displaying received PIM traffic statistics.

tx
Specifies displaying transmitted PIM traffic statistics.

Modes Privileged EXEC mode

Usage Guidelines PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output The **show ipv6 pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the IPv6 PIM interface is configured.
HELLO	The number of IPv6 PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. **NOTE** Unlike PIM dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface. Register Graft (DM)
Err	The total number of MLD messages discarded, including a separate counter for those that failed the checksum comparison.

Examples This example shows PIM traffic statistics:

```
Device# show ipv6 pim traffic
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    0         0           0         0         0         0         0         0
v501    0         0           0         0         0         0         0         0
v503    3302      2524        0         0         0         0         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    3576      0           0         0         0         0         0
v501    1456      0           0         0         0         0         0
v503    1456      1314        0         0         0         2         0
```

This example shows the number of received IPv6 PIM Hello packets dropped on interface 1/1/9 to because an ACL to control neighbor access is configured on it.

```
Device#show ipv6 pim traffic rx
Port    HELLO  JN-PRN  ASSERT  REG      REG       BTSTRP    CAND RP  Err
                               GRFT(DM) STOP(SM)  MSGS(SM)  ADV.(SM)

-------+--------+------+------+------+------+---------+----------+-----
       Rx       Rx      Rx     Rx     Rx        Rx        Rx
Rx
-------+-------+------+------+-------+------+---------+---------+------
e1/1/1  0       0        0      0      0         0         0      0
e1/1/9  924     0        0      0      0         5         0      914
e1/1/12 0       0        0      0      0         0         0      0
v20     0       0        0      0      0         0         0      0
v60     0       0        0      0      0         0         0      0
v310    0       0        0      0      0         0         0      0
v360    0       0        0      0      0         0         0      0
```

History

Release version	Command history
8.0.20a	This command was modified to display, in the Err column, received Hello packets dropped on an interface because of an ACL to control neighbor access.

show ipv6 pimsm-snooping cache

Displays the downstream PIM join/prune information for both source-path tree (SPT) and rendezvous-point tree (RPT).

Syntax **show ipv6 pimsm-snooping cache** [**vlan** *vlan-id*] *ipv6-address* [**resources**]

Parameters *ipv6-address*

Specifies the IP address.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes Privileged exec mode

Command Output The **show ipv6 pimsm-snooping cache** command displays the following information:

Output field	Description
SG	(s,g) downstream fsm state for SPT.
G	(*,g) downstream fsm state for RPT

The **show ipv6 pimsm-snooping cache** command displays the following information only when multi-chassis trunking (MCT) is enabled on the VLAN:

Output field	Description
CCEP	Cluster-client-edge port
CEP	Cluster-edge port
Remote/Local	Join/Prune received on MCT peer or local

Examples The following example shows PIM SM information.

```
Device#show ipv6 pimsm-snooping cache
 OIF Info:
TR - OIF Belongs to Trunk/LAG, Primary port is displayed
SG - (s,g) downstream fsm state:
G - (*,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 503
1    (* ff7e::1:2:3) Up Time: 03:43:40
                   OIF: 1
                   TR(e1/1/4) G : J(183) ET: 210, Up Time: 03:43:40

2    (3000::10 ff7e::1:2:3) Up Time: 00:02:52
                   OIF: 1
                   TR(e1/1/4) SG : J(185) ET: 210, Up Time: 00:02:52
```

The following example shows PIM SM information for a VLAN.

```
Device#show ipv6 pimsm-snooping vlan 503
OIF Info:
TR - OIF Belongs to Trunk/LAG, Primary port is displayed
SG - (s,g) downstream fsm state:
G - (*,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 503
1    (* ff7e::1:2:3) Up Time: 03:43:46
                OIF: 1
                TR(e1/1/4) G : J(177) ET: 210, Up Time: 03:43:46

2    (3000::10 ff7e::1:2:3) Up Time: 00:02:58
                OIF: 1
                TR(e1/1/4) SG : J(179) ET: 210, Up Time: 00:02:58
```

The following example shows PIM SM resource information.

```
Device#show ipv6 pimsm-snooping resources
                     alloc in-use  avail get-fail    limit  get-mem  size init
pimsm group entry     1000      1    999        0   232000        2    64 1000
pimsm source entry    2000      1   1999        0   464000        2    68 2000
pimsm oif entry       2000      1   1999        0   464000        2    89 2000

Total memory in used: 378000 bytes
```

show ipv6 static mroute

Displays information for configured IPv6 multicast routes.

Syntax **show ipv6 static mroute** [**vrf** *vrf-name* | *ipv6-address-prefix/prefix-length*]

Parameters **vrf** *vrf-name*

Specifies a VRF route.

ipv6-address-prefix/prefix-length

Specifies an IPv6 address.

Modes Privileged EXEC mode

Global configuration mode

Usage Guidelines Only resolved and best static mroutes are added to the mRTM table. These routes are prefixed with an asterisk in the output from the **show ipv6 static mroute** command.

Examples Thie following example displays information for configured IPv6 multicast routes:

```
Device(config)# show ipv6 static mroute
IPv6 Static Routing Table - 1 entries:
 IPv6 Prefix                    Interface  Next Hop Router      Met/Dis/Tag Name
*1:1::1:0/120                   ve 90      ::                   1/1/0
```

History

Release version	Command history
8.0.10a	This command was introduced.

show loop-detect no-shutdown-status

Shows the status of interfaces in a loop.

Syntax **show loop-detect no-shutdown-status**

Modes Privileged EXEC mode

Command Output The **show loop-detect no-shutdown-status** command displays the following information:

Output field	Description
Port	The specific interface
Loop status	The duration the port has been in a loop

Examples The following example shows the ports and their loop statuses.

```
device# show loop-detection no-shutdown-status

loop detection no shutdown syslog interval : 5     (unit 1 min /Default 5 min)
loop detection no shutdown port status     :
Note: Port's loop status gets cleared if loop is not detected in a particular
interval window

                Port    ||  Loop Status
       ==================||==========================
        ethernet  1/1/7  ||  (In Loop For 2309 Seconds)
        ethernet  1/1/15 ||  (In Loop For 2309 Seconds
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-auth configuration

Displays the global or interface level MAC authentication configuration.

Syntax **show mac-auth configuration** [**all** | **ethernet** *device/slot/port*]

Parameters

all

Displays the MAC authentication configuration on all interfaces.

ethernet *device/slot/port*

Displays the MAC authentication configuration for a specific interface.

Modes EXEC or Privileged EXEC mode

Global configuration mode

Command Output The **show mac-auth configuration** command displays the following information.

Output field	Description
Status	Displays if MAC authentication is enabled or disabled
Auth-order	The authentication order enabled on the device
Default VLAN	The default VLAN specified on the device
Restricted VLAN	The restricted VLAN specified on the device
Critical VLAN	The critical VLAN specified on the device
Action on Auth failure	The action to be taken on authentication failure
MAC Session Aging	The status of the MAC session aging
Filter Strict Security	The status of filter strict security
Re-authentication	The status of re-authentication
Dot1x Override	The status of dot1x override
Password Override	The status of password override
Password Format	The configured password format
Reauth-period	The re-authentication period specified in seconds
Session max sw-age	The maximum software age configured on the device
Session max hw-age	The maximum hardware age configured on the device

The **show mac-auth configuration all** | **ethernet***device/slot/port* command displays the following information.

Output field	Description
Auth Order	Displays the authentication order
Action on Auth failure	Displays the action to be taken on authentication failure
Action on Auth timeout	Displays the action to be taken on authentication timeout

Output field	Description
Filter Strict Security	Displays if filter strict security is enabled or disabled
DoS Protection	Displays if DoS protection is enabled or disabled
Source-guard Protection	Displays if Source-Guard Protection is enabled or disabled
Aging	Displays if aging is enabled or disabled
Max-sessions	Displays the count of the maximum sessions
Ingress-filtering	Displays if ingress filtering is enabled or disabled

Examples The following example displays the system level MAC authentication configuration.

```
device# show mac-authentication configuration

Status : Enabled
Auth Order : dot1x mac-auth
Default VLAN : 4
Restricted VLAN : Not configured
Critical VLAN : Not configured
Action on Auth failure : Block traffic
MAC Session Aging : Enabled
Filter Strict Security : Enabled
Re-authentication : Enabled
Dot1x Override : Disabled
Password Override : Disabled
Password Format : xxxx.xxxx.xxxx
Reauth-period : 600 seconds
Session max sw-age : 120 seconds
Session max hw-age : 70 seconds
```

The following example displays the MAC authentication configuration for port 1/1/15.

```
device# configure terminal
device(config)# show mac-auth configuration 1/1/15

Port 1/1/15 Configuration:
Auth Order                    : dot1x mac-auth
Action on Auth failure        : Block traffic
Action on Auth timeout        : Treat as a failed authentication
Filter Strict Security        : Enabled
DoS Protection                : Disabled (limit = 512)
Source-guard Protection       : Disabled
Aging                         : Enabled
Max-sessions                  : 32
Auth Filter List (Filter/VLAN) : 1/2
```

The following example displays the MAC authentication information on all interfaces.

```
device# configure terminal
device(config)# show mac-auth configuration all

Port 1/1/1 Configuration:
Auth Order                      : dot1x mac-auth
Action on Auth failure          : Block traffic
Action on Auth timeout          : Treat as a failed authentication
Filter Strict Security          : Enabled
DoS Protection                  : Disabled (limit = 512)
Source-guard Protection         : Disabled
Reauth-timeout                  : 60 seconds
Aging                           : Enabled
Max-sessions                    : 2

Port 1/1/3 Configuration:
Auth Order                      : dot1x mac-auth
Action on Auth failure          : Block traffic
Action on Auth timeout          : Treat as a failed authentication
Filter Strict Security          : Enabled
DoS Protection                  : Disabled (limit = 512)
Source-guard Protection         : Disabled
Reauth-timeout                  : 60 seconds
Aging                           : Enabled
Max-sessions                    : 2
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-auth ip-acl

Shows the layer 3 access lists (ACLs) for MAC authentication.

Syntax **show mac-auth ip-acl** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters

all

Specifies the ACLs at the global level.

ethernet *device*/*slot*/*port*

Specifies the ACLs at the interface level.

Modes Global configuration mode

Interface configuration mode

Examples The **show mac-auth ip-acl** command displays the following information.

```
device(config)# show mac-auth ip-acl all
MAC-Auth IP ACL Information :

Port 1/1/15 : 0010.9400.0010
In-bound IP ACL : 101

Port 1/1/15 : 0010.9400.0020
In-bound IP ACL : 101

Port 2/1/15 : 0015.9400.0020
In-bound IP ACL : 102

device(config)# show mac-auth ip-acl eth 1/1/15
MAC-Auth IP ACL Information :

Port 1/1/15 : 0010.9400.0010
In-bound IP ACL : 101

Port 1/1/15 : 0010.9400.0020
In-bound IP ACL : 101
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-auth sessions

Shows MAC authentication configuration sessions at a global and interface level.

Syntax **show mac-auth sessions** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters

all

Specifies the sessions at the global level.

ethernet *device*/*slot*/*port*

Specifies the sessions at the interface level.

Modes

Privileged EXEC mode

Global configuration

Interface configuration

Command Output

The **show mac-auth sessions** command displays the following information:

Output field	Description
Port	The port number.
MAC Address	The MAC address of the client.
IP Address	The IP address of the client.
VLAN	The VLAN
Auth State	The authentication state.
ACL	The specific ACL applied.
Age	The age of the session.

Examples

The following example displays MAC sessions for all interfaces.

```
device# show mac-auth sessions all
--------------------------------------------------------------------------------

Port  MAC            IP               Vlan   Auth        ACL      Age
      Addr           Addr                    State
--------------------------------------------------------------------------------
1/1/15 0010.9400.0010  192.85.10.1     20   Yes     in-101
1/1/15 0010.9400.0020  192.85.20.1     20   Yes     in-101
2/1/15 0015.9400.0020  192.85.30.1     30   Yes     in-102
```

The following example displays MAC sessions for a specified interface.

```
device# show mac-auth sessions ethernet 1/1/15
--------------------------------------------------------------------------------

Port  MAC            IP               Vlan   Auth        ACL      Age
      Addr           Addr                    State
--------------------------------------------------------------------------------
1/1/15 0010.9400.0010  192.85.10.1     20   Yes     in-101
1/1/15 0010.9400.0020  192.85.20.1     20   Yes     in-101
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-auth statistics

Displays the MAC authentication statistics.

Syntax **show mac-auth statistics** { **all** | **ethernet** *device*/*slot*/*port* }

Parameters **all**

Displays the MAC authentication statistics for all interfaces.

ethernet *device*/*slot*/*port*

Displays the MAC authentication statistics for the specified interface.

Modes Privileged EXEC mode

Command Output The **show mac-auth statistics** command displays the following information:

Output field	Description
Accepted sessions	Number of accepted sessions
Rejected sessions	Number of rejected sessions
Inprogress sessions	Number of inprogress sessions
Attempted sessions	Number of attempted sessions
Number of errors	The number of errors.

Examples The following example displays MAC authentication statistics for all interfaces.

```
device# show mac-auth statistics all

Port 1/1/15 Statistics:
Accepted Sessions       :    2
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0

Port 2/1/15 Statistics:
Accepted Sessions       :    1
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0
```

The following example displays MAC authentication statistics for Ethernet interface 1/1/15.

```
device# show mac-auth statistics ethernet 1/1/15

Port 1/1/15 Statistics:
Accepted Sessions       :    2
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0
```

History

Release version	Command history
08.0.20	This command was introduced.

show macsec statistics ethernet

Displays status information and secure channel statistics for the designated MACsec interface.

Syntax **show macsec statistics ethernet** *device*/*slot*/*port*

Parameters *device*/*slot*/*port*

Interface for which MACsec status information is to be displayed. The interface is designated by device number in stack/slot on the device/interface on the slot.

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

dot1x-mka configuration mode

dot1x-mka-interface configuration mode

Usage Guidelines This command is supported only on the ICX 6610.

It is recommended that you use the **clear macsec ethernet** command to clear previous results for the **show macsec statistics ethernet** command before re-executing it.

Command Output The **show macsec statistics ethernet** command displays the following information:

Output field	Description
Interface (Device/slot/port)	The information that follows describes the designated interface.
Replay Protection (Enabled, Disabled)	Indicates whether replay protection is applied on the interface.
Replay Window (0 through 127)	If out-of-order packets are allowed, indicates allowable window within which an out-of-order packet can be received.
Frame Validation (Enabled, Disabled)	Indicates whether MACsec frame headers are checked.
Secure Channel Statistics:	The fields that follow describe activity on a secure channel established over the designated interface.
TxPktProtectedOnly	Number of transmitted packets with integrity protection only.
TxOctetProtectedOnly	Number of bytes transmitted in packets with integrity protection only.
TxPktEncrypted	Number of transmitted packets that are encrypted.
TxOctetEncrypted	Number of bytes transmitted in encrypted packets.
TxPktMiss	Number of transmitted packets that are neither encrypted nor protected by integrity check.
TxOctetMiss	Number of bytes transmitted in packets that are neither encrypted nor protected by integrity checking.
TxPktDrop	Number of packets dropped at transmission because SAK has been exhausted.
TxPktBad	Number of transmitted packets marked as bad.

Output field	Description
RxPktDecryptedAuth	Number of packets received, decrypted, and checked for integrity protection.
RxOctetTotal	Number of bytes received.
RxOctetAuthOnly	Number of bytes received with Integrity protection only.
RxOctetDecrypted	Number of bytes received and decrypted.
RxPktFailReplayCheck	Number of packets received out of order.
RxPktFailICVCheck	Number of packets received that failed Integrity checking.
RxPktNoMACsecTag	Number of packets received without a MACSec Tag.
RxPktFrameValFail	Number of packets received that failed MACsec frame validation.
RxPktMiss	Number of packets received that did not find a key for decryption.
RxOctetMiss	Number of bytes received that did not find a key for decryption.
RxPktDrop	Number of received packets that were dropped.

Examples

The following code sample shows details for Ethernet interface 1/3/1 (device 1, slot 3, port 1). The interface is verifying MACsec frames and is providing strict replay protection. Based on counter statistics, transmitted packets are being encrypted. A smaller number of packets have been received, have passed integrity checking, and have been decrypted. No packets have been received out of order, and no packets have been dropped. No packets have failed integrity checking. A number of packets have been received without MACsec headers, and numerous bytes did not have a decryption key.

```
device(config-dot1x-mka-1/3/1)# clear macsec ethernet 1/3/1
device(config-dot1x-mka-1/3/1)# show macsec statistics ethernet 1/3/1

Interface                : 1/3/1

Replay Protection   : Enabled
Replay Window       : 0
Frame Validation    : Check

Secure Channel Statistics:
     TxPktProtectedOnly     165074761   TxOctetProtectedOnly          20491766144
         TxPktEncrypted             0       TxOctetEncrypted                    0
              TxPktMiss             0            TxOctetMiss                    0
              TxPktDrop             0               TxPktBad                    0

     RxPktDecryptedAuth          3455          RxOctetTotal                257506
        RxOctetAuthOnly        230740       RxOctetDecrypted                    0
   RxPktFailReplayCheck             0      RxPktFailICVCheck                    0
       RxPktNoMACsecTag           414      RxPktFrameValFail                    0
              RxPktMiss           414            RxOctetMiss                26766
              RxPktDrop             0
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was modified. The **show macsec ethernet** command was changed to **show macsec statistics ethernet** command.

show notification-mac

Displays whether MAC-notification for SNMP traps is enabled or disabled.

Syntax **show notification-mac**

Modes Privileged EXEC mode

Usage Guidelines You can view statistics such as the configured interval, the number of traps sent, and the number of events sent.

Examples The following example displays the MAC-notification statistics:

```
device# show notification-mac
Mac-notification SNMP trap is ENABLED
Configured Interval: 40 seconds
Number of trap messages sent: 2
Number of mac-notification events sent: 20
```

History

Release version	Command history
08.0.10	This command was introduced.

show openflow

Displays the configured OpenFlow parameters.

Syntax **show openflow**

Modes EXEC and Privileged EXEC mode

Global configuration mode

Command Output The **show openflow** command displays the following information:

Output field	Description
Administrative Status	Enable or disable status
Controller Type	OpenFlow 1.0 or OpenFlow1.3 controller
Controller	Number of controllers

Examples

```
device#show openflow

Administrative Status:       Enabled
Controller Type:             OFV 130
Number of Controllers: 4

Controller 1:
Connection Mode:             passive, TCP
Listening Address:           0.0.0.0
Connection Port:             6633
Connection Status:           TCP_LISTENING
Role:                           Equal
Asynchronous Configuration:  Packet-in (no-match|action|invalid-ttl)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-
delete)

Controller 2:
Connection Mode:             active, TCP
Controller Address:          10.25.128.243
Connection Port:             2001
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Master
Asynchronous Configuration:  Packet-in (no-match|action|invalid-ttl)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-
delete)
Controller 3:
Connection Mode:             active, TCP
Controller Address:          10.25.128.242
Connection Port:             6633
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Slave
Asynchronous Configuration:  Port-status (add|delete|modify)

Controller 4:
Connection Mode:             active, TCP
Controller Address:          10.25.128.250
Connection Port:             2002
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Slave
Asynchronous Configuration:  Port-status (add|delete|modify)

Match Capability:
Port, Destination MAC, Vlan, Vlan PCP
Openflow Enabled Ports:      e1/1 e1/2
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow controller

Displays the controller information in a flow.

Syntax **show openflow controller**

Modes EXEC and Privileged EXEC mode

Global configuration mode

Command Output The **show openflow controller** command displays the following information:

Output field	Description
Mode	Gives the active and passive connection of the controller.
IP address	IP address of the port
Port	Port number
Status	After the connection and OpenFlow handshake, the controller gives the role of OpenFlow channel.
Role	Equal, Master and Slave role for the controller.

Examples

```
device# show openflow controller
------------------------------------------------------------------------
Contlr Mode  TCP/SSL IP-address     Port       Status            Role
------------------------------------------------------------------------
1   (Equal)    passive  TCP    0.0.0.0          6633   TCP_LISTENING
2   (Master)   active   TCP    10.25.128.179    6633   OPENFLOW_ESABLISHED
3   (Slave)    active   TCP    10.25.128.177    6633   OPENFLOW_ESABLISHED
3   (Equal)    active   TCP    10.25.128.165    6633   OPENFLOW_ESABLISHED
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow flows

Displays the flows information on the OpenFlow ports.

Syntax **show openflow flows**

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output The **show openflow flows** command displays the following information:

Output field	Description
Flow	Number of flows
Packet	Total Number of data packets trapped to be sent to controller
Byte	Total Number of data bytes trapped to be sent to controller

Examples This command displays the output for flows.

```
device# show openflow flows

Total Number of data packets sent to controller:                    0
Total Number of data bytes sent to controller  :                    0

Total Number of Flows: 1
        Total Number of Port based Flows: 1
        Total Number of L2 Generic Flows: 0
        Total Number of L3 Generic Flows: 0
    ……...
    ……

Flow ID: 1 Priority: 32768 Status: Active
        Rule:
           In Port:      e2/5
        Instructions: Apply-Actions
                Action: FORWARD
                        Out Port:  e2/1
                Meter id: 1023
        Statistics:
           Total Pkts: 0
           Total Bytes: 0
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow groups

Displays the maximum number of actions in a bucket, the maximum number of buckets in a group and the maximum number of groups.

Syntax **show openflow groups** *group-id*

Parameters **groups** *group-id*

Shows details of a specific OpenFlow group.

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output The **show openflow groups** command displays the following information:

Output field	Description
Group	Maximum number of group in a flow
Bucket	Number of bucket per group
Action	Number of action per bucket

Examples

```
device#show openflow groups

Max number of groups             : 512
Max number of buckets per group  :  64
Max number of actions per bucket :   1

Max number of SELECT groups          : 120
Max number of buckets in SELECT group: 8
Starting Trunk ID for SELECT groups  : 257
Group id 1

  Transaction id        4043243760
  Type                  ALL
  Packet Count          0
  Byte   Count          0
  Flow   Count          0
  Number of buckets     2
bucket #1
    Weight             0
    Number of actions   1
      action 1: out port: 2/3

  bucket #2
    Weight             0
    Number of actions   1
      action 1: out port: 2/4

----

Total no. of entries printed: 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow interfaces

Displays the information about the interfaces in a OpenFlow flow.

Syntax **show openflow interfaces**

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

Command Output The **show openflow interfaces** command displays the following information:

Output field	Description
Port	Port Number
Link	Link status
Speed	Configured speed
Tag	Tag status
Mac Address	MAC address of the port
Mode	Gives the information about the layers

Examples

```
device# openflow enable layer3 hybrid
device# show openflow interfaces

Total number of Openflow interfaces: 5

Port  Link     Speed Tag MAC            OF-portid Name    Mode
1/1   Up       1G    Yes 000c.dbf5.bd00 1                 Layer2
1/2   Up       1G    Yes 000c.dbf5.bd01 2                 Layer2
1/3   Up       1G    Yes 000c.dbf5.bd01 3                 Hybrid-Layer3
1/4   Up       1G    Yes 000c.dbf5.bd01 4                 Hybrid-Layer3
1/5   Up       1G    Yes 000c.dbf5.bd01 5                 Hybrid-Layer3
```

This command displays information for a particular interface on a specific slot and port..

```
device# show interface ethernet 1/1/6

GigabitEthernet1/1/6 is up, line protocol is up
  Port up for 51 minutes 53 seconds
  Hardware is GigabitEthernet, address is 748e.f8e7.d901 (bia 748e.f8e7.d901)
  Configured speed auto, actual 1Gbit, configured duplex fdx, actual fdx
  Configured mdi mode AUTO, actual MDI
  Member of L2 VLAN ID 100, port is untagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0, mac-learning is enabled
  OpenFlow enabled, Openflow Index 1, Flow Type Layer2
  Flow Control is config enabled, oper enabled, negotiation disabled
  Mirror disabled, Monitor disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  Inter-Packet Gap (IPG) is 96 bit times
  MTU 1500 bytes, encapsulation ethernet
  300 second input rate: 3904 bits/sec, 7 packets/sec, 0.00% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  23153 packets input, 1530094 bytes, 0 no buffer
  Received 1721 broadcasts, 21432 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  0 packets output, 0 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 0 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled

Egress queues:
Queue counters    Queued packets    Dropped Packets
    0                   0                   0
    1                   0                   0
    2                   0                   0
    3                   0                   0
    4                   0                   0
    5                   0                   0
    6                   0                   0
    7                   0                   0
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow meters

Displays all the meters in a OpenFlow flow.

Syntax **show openflow meters** *meter-id*

Parameters **meters** *meter-id*

Shows details of a specific OpenFlow meter.

Modes User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output The **show openflow meters** command displays the following information:

Output field	Description
Meter-id	Meter number
Band	Number of bands in a meter
Band type	Band type (supported type: Drop, DSCP_REMARK)
Rate	Rate of the band
Counter	Band specific counter

Examples The following example displays output with single meter band.

```
device(config)# show openflow meters 1
Meter id: 1

  Transaction id:        1437
  Meter Flags:            KBPS BURST STATS
  Flow Count:            0
  Number of  bands:      1
  In packet count:       -NA-
  In byte count:         0

  Band Type:    DROP

    Rate:                         750000
    Burst size:                   1500          kb
    In packet band count:         -NA-
    In byte band count:           0
```

The following example displays output with two meter bands.

```
device(config)# show openflow meters 2
Meter id: 2

  Transaction id:        1438
  Meter Flags:            KBPS BURST STATS
  Flow Count:            0
  Number of  bands:      2
  In packet count:       -NA-
  In byte count:         0

  Band Type:    DSCP-REMARK

    Rate:                          750000
    Burst size:                    1500          kb
    Prec level:                    1
    In packet band count:          -NA-
    In byte band count:            0


  Band Type:    DROP

    Rate:                          1000000
    Burst size:                    2000          kb
    In packet band count:          -NA-
    In byte band count:            0
```

History

Release version	Command history
08.0.20	This command was introduced.

show packet-inerror-detect

Displays details related to the monitoring for inError packets for configured ports.

Syntax **show packet-inerror-detect**

Modes Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines Use this show command to view details related to the monitoring of inError packets for configured ports.

Command Output The **show packet-inerror-detect** command displays the following information:

Output field	Description
Sampling interval	Displays the configured sampling interval.
Port	Identifies a port.
Packet inError count	The number of inError packets received in the sampling interval for the specific port.
State	Displays the status for the specific port.

Examples The following example displays details related to the monitoring for inError packets for configured ports.

```
device# show packet-inerror-detect

Sampling interval 5 secs

Port    Packet inError count State
1/1/1   30                   Operational
1/1/37  10                   ERR-DISABLED
2/1/1   100                  Operational
```

History

Release version	Command history
07.3.00g	This command was introduced.

show priority-flow-control

Displays the priority flow control (PFC) on the system.

Syntax **show priority-flow-control**

Modes Privileged EXEC mode

Examples The following example shows the PFC status of all priority groups.

```
Device# show priority-flow-control

Global PFC Status: Enabled
PFC Enabled on PG0
PFC Disabled on PG1
PFC Disabled on PG2
PFC Disabled on PG3
```

The following example shows the PFC status disabled.

```
Device# show priority-flow-control

Global PFC Status: Disabled
```

History

Release version	Command history
8.0.10	This command was introduced.

show qos egress-buffer-profile

Displays information about egress buffer profiles.

Syntax **show qos egress-buffer-profile** [*user-profile-name* | **all**]

Parameters *user-profile-name*

Displays information for the specified egress buffer profile.

all

Displays information for all egress buffer profiles configured in the system and a list of all ports attached to any egress buffer profile.

Modes Global configuration mode

Examples The following example displays information for an egress buffer profile named egress1.

```
Device(config)# show qos egress-buffer-profile egress1

Egress Buffer Profile: egress1
Ports attached:  1/1/2
Per Queue Details:       Share Level:
Queue 0                  level4-1/9
Queue 1                  level3-1/16
Queue 2                  level3-1/16
Queue 3                  level3-1/16
Queue 4                  level3-1/16
Queue 5                  level3-1/16
Queue 6                  level3-1/16
Queue 7                  level2-1/32
```

History

Release version	Command history
8.0.10	This command was introduced.

show qos ingress-buffer-profile

Displays information about ingress buffer profiles.

Syntax **show qos ingress-buffer-profile** [*user-profile-name* | **all**]

Parameters *user-profile-name*

Displays information for the specified ingress buffer profile.

all

Displays information for all the ingress buffer profiles configured in the system and a list of their XOFF threshold levels.

Modes Global configuration mode

Examples The following example displays information for all the ingress buffer profiles configured in the system and their XOFF threshold levels.

```
Device(config)# show qos ingress-buffer-profile all

Ingress Buffer Profile: i1
Ports attached:  1/1/1
Per PG Detail:           XOFF Level:
PG 0                     level1-1/64
PG 1                     level3-1/16
PG 2                     level4-1/9
PG 3                     level5-1/5

Ingress Buffer Profile: ing1
Ports attached:  --
Per PG Detail:           XOFF Level:
PG 0                     level6-1/3
PG 1                     level2-1/32
PG 2                     level2-1/32
PG 3                     level2-1/32
```

History

Release version	Command history
8.0.20	This command was introduced.

show qos-internal-trunk-queue

Displays the queue-share level of inter-packet-processor (inter-pp) links used to connect master and slave units in ICX 7450 devices.

Syntax **show qos-internal-trunk-queue**

Modes Global configuration mode

Examples The following example displays the queue-share level applied on egress queues of inter-pp links in a system.

```
device(config)#show qos-internal-trunk-queue
Per Queue Details:       Share Level:
Queue 0                  level7-1/2
Queue 1                  level3-1/16
Queue 2                  level3-1/16
Queue 3                  level3-1/16
Queue 4                  level3-1/16
Queue 5                  level3-1/16
Queue 6                  level3-1/16
Queue 7                  level3-1/16
```

History

Release version	Command history
08.0.20	This command was introduced.

show qos priority-to-pg

Displays priority-to-priority-group (PG) mapping for priority flow control (PFC).

Syntax **show qos priority-to-pg**

Modes Global configuration mode

Usage Guidelines This command displays priority-to-PG mapping for the following flow control modes:

- PFC
- Symmetrical flow control
- Asymmetrical flow control

Examples The following example shows priority-to-PG mapping for PFC.

```
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 0
QoS Internal Priority 1 mapped to Priority Group 0
QoS Internal Priority 2 mapped to Priority Group 1
QoS Internal Priority 3 mapped to Priority Group 1
QoS Internal Priority 4 mapped to Priority Group 1
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example shows priority-to-PG mapping for 802.3x (Flow-Control). Honor is enabled.

```
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 0
QoS Internal Priority 1 mapped to Priority Group 0
QoS Internal Priority 2 mapped to Priority Group 1
QoS Internal Priority 3 mapped to Priority Group 1
QoS Internal Priority 4 mapped to Priority Group 1
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example shows priority-to-PG mapping for symmetrical flow control for 802.3x (Flow-Control) in Both mode (Generate and Honor are enabled) or Generate-only mode.

```
Device(config)# symmetrical-flow-control enable
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 7
QoS Internal Priority 1 mapped to Priority Group 7
QoS Internal Priority 2 mapped to Priority Group 7
QoS Internal Priority 3 mapped to Priority Group 7
QoS Internal Priority 4 mapped to Priority Group 7
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example enables flow control on all priorities and shows the priority-to-PG mapping.

```
Device(config)# symmetrical-flow-control enable all
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 7
QoS Internal Priority 1 mapped to Priority Group 7
QoS Internal Priority 2 mapped to Priority Group 7
QoS Internal Priority 3 mapped to Priority Group 7
QoS Internal Priority 4 mapped to Priority Group 7
QoS Internal Priority 5 mapped to Priority Group 7
QoS Internal Priority 6 mapped to Priority Group 7
QoS Internal Priority 7 mapped to Priority Group 4
```

History

Release version	Command history
8.0.10	This command was introduced.

show qos-profiles

Displays information about QoS profiles

Syntax **show qos-profiles** { **all** | *name* }

Parameters **all**

Displays information for all profiles.

name

Displays information for the specified profile.

Modes Global configuration mode

Examples The following example displays information for all the queues on an FSX device.

```
Device# show qos-profiles all
bandwidth scheduling mechanism: weighted priority
Profile qosp7     : Priority7   bandwidth requested  25% calculated  25%
Profile qosp6     : Priority6   bandwidth requested  15% calculated  15%
Profile qosp5     : Priority5   bandwidth requested  12% calculated  12%
Profile qosp4     : Priority4   bandwidth requested  12% calculated  12%
Profile qosp3     : Priority3   bandwidth requested  10% calculated  10%
Profile qosp2     : Priority2   bandwidth requested  10% calculated  10%
Profile qosp1     : Priority1   bandwidth requested  10% calculated  10%
Profile qosp0     : Priority0   bandwidth requested   6% calculated   6%
```

The following example displays information, including multicast queue weights, for all the queues on an ICX 7450 device.

```
Device#show qos-profiles all
bandwidth scheduling mechanism: mixed weighted priority with strict priority
Unicast Traffic
Profile qosp7     : Priority7(Highest) Set as strict priority
Profile qosp6     : Priority6          Set as strict priority
Profile qosp5     : Priority5          bandwidth requested  25% calculated  25%
Profile qosp4     : Priority4          bandwidth requested  15% calculated  15%
Profile qosp3     : Priority3          bandwidth requested  15% calculated  15%
Profile qosp2     : Priority2          bandwidth requested  15% calculated  15%
Profile qosp1     : Priority1          bandwidth requested  15% calculated  15%
Profile qosp0     : Priority0(Lowest)  bandwidth requested  15% calculated  15%
Multicast Traffic
Profile qosp7+qosp6                     : Priority7(Highest),6      Set as strict
priority
Profile qosp5                           : Priority5                 bandwidth
requested  25% calculated  25%
Profile qosp4+qosp3+qosp2               : Priority4,3,2             bandwidth
requested  45% calculated  45%
Profile qosp1+qosp0                     : Priority1,0(Lowest)       bandwidth
requested  30% calculated  30%
```

History

Release version	Command history
08.0.20	This command was modified to display information for multicast queue weights on ICX 7450 and ICX 7750 devices.

show qos scheduler-profile

Displays information about scheduler profiles.

Syntax **show qos scheduler-profile** { **all** *user-profile-name*}

Parameters **all**

Displays information for all the scheduler profiles configured in the system and a list of all the ports attached to any scheduler profile.

user-profile-name

Displays information for the specified scheduler profile only.

Modes Global configuration mode

Usage Guidelines A scheduler profile must be configured before it can be displayed.

Information can be displayed for a maximum of eight scheduler profiles.

On ICX 7750 and ICX 7450 devices this command also displays information for multicast queue weights.

Examples The following example displays information for a scheduler profile named user1.

```
Device(config)# show qos scheduler-profile user1

User Scheduler Profile: user1   Scheduling Option: Weighted round-robin
Ports attached:  1/1/1
Per Queue details:    Bandwidth%
Traffic Class 0            1%
Traffic Class 1            1%
Traffic Class 2           10%
Traffic Class 3           10%
Traffic Class 4           10%
Traffic Class 5           10%
Traffic Class 6           20%
Traffic Class 7           38%
```

The following example displays information for all the scheduler profiles configured in the system.

```
Device(config)# show qos scheduler-profile all

User Scheduler Profile: user1   Scheduling Option: Weighted round-robin
Ports attached:  1/1/1
Per Queue details:    Bandwidth%
Traffic Class 0             1%
Traffic Class 1             1%
Traffic Class 2            10%
Traffic Class 3            10%
Traffic Class 4            10%
Traffic Class 5            10%
Traffic Class 6            20%
Traffic Class 7            38%

User Scheduler Profile: user2   Scheduling Option: Strict scheduling
Ports attached:  --

User Scheduler Profile: user3   Scheduling Option: Mixed-SP-WRR
Ports attached:  --
Per Queue details:    Bandwidth%
Traffic Class 0            15%
Traffic Class 1            15%
Traffic Class 2            15%
Traffic Class 3            15%
Traffic Class 4            15%
Traffic Class 5            25%
Traffic Class 6            sp
Traffic Class 7            sp

User Scheduler Profile: user4   Scheduling Option: Weighted round-robin
Ports attached:  --
Per Queue details:    Bandwidth%
Traffic Class 0             3%
Traffic Class 1             3%
Traffic Class 2             3%
Traffic Class 3             3%
Traffic Class 4             3%
Traffic Class 5             3%
Traffic Class 6             7%
Traffic Class 7            75%
```

The following example displays information, including multicast queue weights, for a scheduler profile named profle1 on ICX 7450 anf ICX 7750 devices.

```
Device(config)# show qos scheduler-profile profile1
User Scheduler Profile: profile1     Scheduling Option: Weighted round-robin
Unicast per Queue details:      Bandwidth%
Traffic Class 0                      8%
Traffic Class 1                      8%
Traffic Class 2                      8%
Traffic Class 3                      8%
Traffic Class 4                      8%
Traffic Class 5                      8%
Traffic Class 6                      8%
Traffic Class 7                     44%
Multicast per Queue details:    Bandwidth%
Traffic Class 0,1                   16%
Traffic Class 2,3,4                 24%
Traffic Class 5                      8%
Traffic Class 6,7                   52%
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified to display information for multicast queue weights on ICX 7450 and ICX 7750 devices.

show rmon

Displays the Remote monitoring (RMON) agent status and information about RMON alarms, events, history, logs, and statistics on the interface.

Syntax **show rmon** { **alarm** *alarm-number* | **event** *event-number* | **history** *history-index* | **logs** *event-index* | **statistics** [*number* | *interface-type* | *interface-number*] }

Parameters

alarm
Specifies to display the RMON alarm table.

alarm-number
Specifies the alarm index identification number. Valid values range from 1 through 65535.

event
Specifies to display the RMON event table.

event-number
Specifies the event index identification number. Valid values range from 1 through 65535.

history
Specifies to display the history control data entries for port or interface.

history-number
Specifies the history index identification number of the history entry.

logs
Specifies to display the RMON logging table where RMON log entries are stored.

event-index
Specifies the event index identification number. Valid values range from 1 through 65535.

statistics
Specifies to display the RMON Ethernet statistics; and the statistics group that collects statistics on promiscuous traffic across an interface and total traffic into and out of the agent interface. Valid values range from 1 through 65535.

statistics-number
Specifies the statistics index identification number of the statistics entry.

interface-type
Specifies the ethernet interface or management port.

interface-number
Specifies the interface or management port number.

Modes Privileged EXEC mode

Global configuration mode

Command Output The **show rmon** command displays the following information:

Output field	Description
Rising threshold	The sampling value limit, beyond which the rising alarm is triggered.
Falling threshold	The sampling value limit, beyond which the falling alarm is triggered.

Output field	Description
Octets	The total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Drop events	Indicates an overrun at the port. The port logic could not receive the traffic at full line rate and had to drop some packets as a result. The counter indicates the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.
Packets	The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Broadcast pkts	The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Multicast pkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC align errors	The total number of packets received that were from 64 - 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The packet length does not include framing bits but does include FCS octets.
Undersize pkts	The total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Fragments	The total number of packets received that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for this counter to increment, since it counts both runts (which are normal occurrences due to collisions) and noise hits. This number does not include framing bits but does include FCS octets.
Oversize packets	The total number of packets received that were longer than 1518 octets and were otherwise well formed. This number does not include framing bits but does include FCS octets. **NOTE** 48GC modules do not support count information on oversized packets and report 0.

Output field	Description
Jabbers	The total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **NOTE** This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. This number does not include framing bits but does include FCS octets. **NOTE** 48GC modules do not support count information on jabbers and report 0.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 octets pkts	The total number of packets received that were 64 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
65 to 127 octets pkts	The total number of packets received that were 65 - 127 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
128 to 255 octets pkts	The total number of packets received that were 128 - 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
256 to 511 octets pkts	The total number of packets received that were 256 - 511 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
512 to 1023 octets pkts	The total number of packets received that were 512 - 1023 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
1024 to 1518 octets pkts	The total number of packets received that were 1024 - 1518 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Event Index	The event index identification number.
Log Index	The log index identification number.
Log Generated time	The time at which the log is generated.
Log Description	Indicates the type of alarm; whether it is a rising or falling alarm.

Examples The following example shows the output of the **show rmon alarm** command.

```
device(config)# show rmon alarm
Alarm 1 is active, owned by monitor
 Monitors etherStatsPkts.13 every 5 seconds
 Taking absolute samples, last value was 675
 Rising threshold is 100, assigned to event 1
 Falling threshold is 0, assigned to event 1
 On startup enable rising or falling alarm

Alarm 2 is active, owned by monitor
 Monitors etherStatsPkts.2 every 5 seconds
 Taking absolute samples, last value was 414
 Rising threshold is 100, assigned to event 3
 Falling threshold is 0, assigned to event 3
 On startup enable rising or falling alarm
```

The following example shows the output of the **show rmon event** command.

```
device(config)# show rmon event
Event 1 is active, owned by monitor
 Description is testing
 Event firing causes log, community
 Batch ID 0, argument <none>
 Last fired at system up time 3 minutes 52 seconds

Event 2 is active, owned by monitor
 Description is logging
 Event firing causes log and trap, community public
 Batch ID 0, argument <none>
 Last fired at system up time 8 minutes 12 seconds
```

The following example shows the output of the **show rmon history** *history-index* command.

```
device(config)# show rmon history 1
History 1 is active, owned by monitor
 Monitors interface mgmt1 (ifIndex 25) every 30 seconds
 25 buckets were granted to store statistics
```

The following example shows the output of the **show rmon logs** command.

```
device(config)# show rmon logs
 Event Index = 1
     Log Index = 1
     Log Generated time = 00:03:52 (23200)
     Log Description  = rising alarm

 Event Index = 2
     Log Index = 1
     Log Generated time = 00:08:12 (49200)
     Log Description  = rising alarm

 Event Index = 3
     Log Index = 1
     Log Generated time = 00:05:12 (31200)
     Log Description  = rising alarm

 Event Index = 4
     Log Index = 1
     Log Generated time = 00:01:32 (9200)
     Log Description  = falling alarm

     Log Index = 2
     Log Generated time = 00:02:52 (17200)
     Log Description  = rising alarm
```

The following example shows the output of the **show rmon logs** *event-index* command.

```
device(config)# show rmon logs 2
Event Index = 2
     Log Index = 1
     Log Generated time = 00:08:12 (49200)
     Log Description  = rising alarm
```

The following example shows the output of the **show rmon statistics** *number* command.

```
device(config)# show rmon statistics 1
Ethernet statistics 1 is active, owned by monitor
 Interface 1/1/1 (ifIndex 1) counters
           Octets                    0
      Drop events                    0            Packets                    0
    Broadcast pkts                   0      Multicast pkts                   0
 CRC align errors                    0      Undersize pkts                   0
    Oversize pkts                    0           Fragments                   0
          Jabbers                    0          Collisions                   0

 Packet size counters
               64                    0           65 to 127                   0
       128 to 255                    0          256 to 511                   0
      512 to 1023                    0        1024 to 1518                   0
```

The following example shows the statistics of the ethernet interface 1/2/1.

```
device(config)# show rmon statistics ethernet 1/2/1
Ethernet statistics 65 is active, owned by monitor
 Interface 1/2/1 (ifIndex 65) counters
           Octets          30170677670
      Drop events                    0            Packets             72281139
    Broadcast pkts                   0      Multicast pkts             66309417
 CRC align errors                    0      Undersize pkts                   0
    Oversize pkts                    0           Fragments                   0
          Jabbers                    0          Collisions                   0

 Packet size counters
               64                    0           65 to 127            10703415
       128 to 255             19353559          256 to 511            18658554
      512 to 1023             17980963        1024 to 1518             5584648
```

History

Release version	Command history
08.0.20	The **logs** keyword was introduced.

show running interface

Displays information about the interface.

Syntax **show running interface** [**ethernet** *stack/slot/port* [**to ethernet** *stack/slot/port*] | **loopback** *loopback-number* | **management** *por-id* | **tunnel** *tunnel-id* | **ve** *ve-number*]

Parameters

ethernet *stack/slot/port*

Specifies the configuration on a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

to

Specifies information for a range of physical interfaces.

loopback *loopback-number*

Specifies information for a loopback interface.

management *port-id*

Specifiesinformation for a management port.

tunnel *tunnel-id*

Specifies information for a tunnel interface.

ve *ve-number*

Specifies information for a virtual interface.

Modes Privileged EXEC mode

Examples The following example displays output from the **show running interface** command, showing that ACLs 10 and f10 are applied to interface 1/1/9 to control neighbor access.

```
Device#show running interface ethernet 1/1/9
interface ethernet 1/1/9
 ip address 15.1.1.5 255.255.255.0
 ip pim-sparse
 ip pim neighbor-filter 10
 ip ospf area 0
 ipv6 address 201::1/64
 ipv6 ospf area 0
 ipv6 pim-sparse
 ipv6 pim neighbor-filter f10
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show span designated-protect

Displays a list of all ports that are not allowed to go into the designated forwarding state.

Syntax **show span designated-protect**

Modes Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples The following example indicates that the designated forwarding state is disallowed for interfaces 2/1/7, 2/1/19, and 2/2/3.

```
device(config)# show span designated-protect
Designated Protection Enabled on:
Ports: (U2/M1)   7 19
Ports: (U2/M2)   3
```

History

Release version	Command history
07.3.00g	This command was introduced.

show stack

Displays information about the units in a stack and a representation of the stack topology.

Syntax **show stack** *num*

Parameters ***num***

Displays information for the specified stack unit ID.

Modes Privileged EXEC mode

Command Output The **show stack** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
Type	Specifies the type (model) of the stack unit.
Role	Specifies the role of the stack unit. The roles are controller, standby, or member.
Mac Address	Specifies the MAC address of the stack unit. The roles are controller, standby, or member.
Pri	Specifies the priority value assigned to the stack unit. The default value is 128.
State	Specifies whether the stack unit is local or remote. A unit with a State value of Local is the active controller. Units with a State value of Remote are either standby units or member units.
Comment	Indicates if the stack unit is ready (available).

Examples The following example displays information about a stack with six stack trunks, including a representation of the stack topology.

```
device# show stack

T=21h22m31.3: alone: standalone, D: dynamic cfg, S: static, A=10, B=11, C=12
ID   Type          Role    Mac Address    Pri State   Comment
1  S ICX7750-48XGF active  cc4e.246d.9e00 128 local   Ready
2  S ICX7750-48XGF standby cc4e.246d.8d80   0 remote  Ready
3  S ICX7750-48XGF member  cc4e.246d.9b00   0 remote  Ready
4  S ICX7750-48XGF member  cc4e.246d.9c80   0 remote  Ready
5  S ICX7750-20QXG member  cc4e.2439.2a80   0 remote  Ready
6  S ICX7750-20QXG member  cc4e.2439.3700   0 remote  Ready
7  S ICX7750-20QXG member  cc4e.2439.3880   0 remote  Ready
8  S ICX7750-20QXG member  cc4e.2439.2d00   0 remote  Ready
9  S ICX7750-48XGC member  cc4e.2439.1a00   0 remote  Ready
10 S ICX7750-48XGC member  cc4e.2439.1680   0 remote  Ready
11 S ICX7750-48XGC member  cc4e.2439.1d80   0 remote  Ready
12 S ICX7750-48XGC member  cc4e.2439.1280   0 remote  Ready

    active
     +---+        +---+        +---+        +---+        +---+        +---+
 -2/1| 1 |2/4--3/1| C |3/4==2/1| B |2/4==2/1| A |2/4--2/1| 9 |2/4--2/1| 8 |2/4=
|    +---+        +---+        +---+        +---+        +---+        +---+   |
|                                                                              |
|  standby                                                                     |
|    +---+        +---+        +---+        +---+        +---+        +---+   |
-2/4| 2 |2/1==2/4| 3 |2/1--2/4| 4 |2/1==2/4| 5 |2/1--2/4| 6 |2/1==2/4| 7 |2/1=
     +---+        +---+        +---+        +---+        +---+        +---+
Standby u2 - protocols ready, can failover
Current stack management MAC is cc4e.246d.9e00
```

show stack connection

Displays a representation of stack topology and a detailed connection report that contains information on connection errors or hardware failures.

Syntax **show stack connection**

Modes Privileged EXEC mode

Examples The following example displays a representation of a ring topology that has seven stack units and details on each of the trunk link connections.

```
device# show stack connection
Probing the topology. Please wait ...
device#
    active
    +---+        +---+        +---+        +---+        +---+        +---+
=2/1| 4 |2/6==2/6| 3 |2/1==2/1| 2 |2/6==2/6| 1 |2/1==2/1| 7 |2/6==2/6| 6 |2/1=
|   +---+        +---+        +---+        +---+        +---+        +---+   |
|                                                                             |
|                                                                      standby  |
|                                                                       +---+   |
-------------------------------------------------------------------------2/1| 5 |2/6=
                                                                        +---+

trunk probe results: 7 links
Link 1: u7 -- u1, num=5
1: 1/2/1 (T0) <---> 7/2/1 (T0)
2: 1/2/2 (T0) <---> 7/2/2 (T0)
3: 1/2/3 (T0) <---> 7/2/3 (T0)
4: 1/2/4 (T0) <---> 7/2/4 (T0)
5: 1/2/5 (T0) <---> 7/2/5 (T0)
Link 2: u2 -- u1, num=5
1: 1/2/6 (T1) <---> 2/2/6 (T1)
2: 1/2/7 (T1) <---> 2/2/7 (T1)
3: 1/2/8 (T1) <---> 2/2/8 (T1)
4: 1/2/9 (T1) <---> 2/2/9 (T1)
5: 1/2/10(T1) <---> 2/2/10(T1)
Link 3: u3 -- u2, num=5
1: 2/2/1 (T0) <---> 3/2/1 (T0)
2: 2/2/2 (T0) <---> 3/2/2 (T0)
3: 2/2/3 (T0) <---> 3/2/3 (T0)
4: 2/2/4 (T0) <---> 3/2/4 (T0)
5: 2/2/5 (T0) <---> 3/2/5 (T0)
Link 4: u4 -- u3, num=5
1: 3/2/6 (T1) <---> 4/2/6 (T1)
2: 3/2/7 (T1) <---> 4/2/7 (T1)
3: 3/2/8 (T1) <---> 4/2/8 (T1)

4: 3/2/9 (T1) <---> 4/2/9 (T1)
5: 3/2/10(T1) <---> 4/2/10(T1)
Link 5: u5 -- u4, num=5
1: 4/2/1 (T0) <---> 5/2/1 (T0)
2: 4/2/2 (T0) <---> 5/2/2 (T0)
3: 4/2/3 (T0) <---> 5/2/3 (T0)
4: 4/2/4 (T0) <---> 5/2/4 (T0)
5: 4/2/5 (T0) <---> 5/2/5 (T0)
Link 6: u6 -- u5, num=5
1: 5/2/6 (T1) <---> 6/2/1 (T0)
2: 5/2/7 (T1) <---> 6/2/2 (T0)
3: 5/2/8 (T1) <---> 6/2/3 (T0)
4: 5/2/9 (T1) <---> 6/2/4 (T0)
5: 5/2/10(T1) <---> 6/2/5 (T0)
Link 7: u7 -- u6, num=5
1: 6/2/6 (T1) <---> 7/2/6 (T1)
2: 6/2/7 (T1) <---> 7/2/7 (T1)
3: 6/2/8 (T1) <---> 7/2/8 (T1)
4: 6/2/9 (T1) <---> 7/2/9 (T1)
5: 6/2/10(T1) <---> 7/2/10(T1)
CPU to CPU packets are fine between 7 units.
```

show stack detail

Displays information on all units in the stack, including the role, MAC address, priority, status, and stack connections for each stack unit.

Syntax **show stack detail**

Modes Privileged EXEC mode

Command Output The **show stack detail** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
Type	Specifies the type (model) of the stack unit.
Role	Specifies the role of the stack unit. The roles are controller, standby, or member.
Mac Address	Specifies the MAC address of the stack unit. The roles are controller, standby, or member.
Pri	Specifies the priority value assigned to the stack unit. The default value is 128.
State	Specifies whether the stack unit is local or remote. A unit with a State value of Local is the active controller. Units with a State value of Remote are either standby units or member units.
Comment	Indicates if the stack unit is ready (available).
Unit #	Specifies the number assigned to the stack unit. Each unit in the stack has a unique unit number. (This is the same as the ID of the stack unit.)
Stack Port Status	Indicates whether the stack port is connected or disconnected. A port with the up status of up is connected to the stack, and a ports with the status of down (dn) is not connected to the stack.
Neighbors	Indicates units in the stack that are connected together. Each unit in the stack is connected to at least one other stack unit.
System uptime	Indicates the amount of time that the stack unit has been running since the last reset. The System uptime is listed for each unit in the stack.

Examples The following example displays information on a full ICX 7450 stack containing 12 units, with six different models.

```
device# show stack detail

T=17h38m45.2: alone: standalone, D: dynamic cfg, S: static, A=10, B=11, C=12
ID   Type          Role    Mac Address    Pri State   Comment
1  S ICX7450-24G   active  cc4e.246c.ff80 128 local   Ready
2  S ICX7450-24G   standby cc4e.246d.02c8   0 remote  Ready
3  S ICX7450-24G   member  cc4e.246c.ffd0   0 remote  Ready
4  S ICX7450-24P   member  cc4e.246d.0520   0 remote  Ready
5  S ICX7450-48G   member  cc4e.246d.1c78   0 remote  Ready
6  S ICX7450-48G   member  cc4e.246d.1b78   0 remote  Ready
7  S ICX7450-48G   member  cc4e.246d.1df8   0 remote  Ready
8  S ICX7450-48P   member  cc4e.2489.8640   0 remote  Ready
9  S ICX7450-48GF  member  cc4e.246d.1478   0 remote  Ready
10 D ICX7450-24P   member  cc4e.246d.0638   0 remote  Ready
11 D ICX7450-24P   member  cc4e.246d.0778   0 remote  Ready
12 D ICX7450-48P   member  cc4e.246d.2938   0 remote  Ready

    active       standby
      +---+        +---+        +---+        +---+        +---+        +---+
  3/1| 1 |4/1--3/1| 2 |4/1--3/1| 3 |4/1--3/1| 4 |4/1--3/1| 5 |4/1--3/1| 6 |4/1-
     +---+        +---+        +---+        +---+        +---+        +---+   |
                                                                               |
                                                                               |
     +---+        +---+        +---+        +---+        +---+        +---+   |
     | C |3/1--4/1| B |3/1--4/1| A |3/1--4/1| 9 |3/1--4/1| 8 |3/1--4/1| 7 |3/1-
     +---+        +---+        +---+        +---+        +---+        +---+
Will assign standby in 53 sec due to all ready

Standby u2 - wait for standby assignment due to election
Current stack management MAC is cc4e.246c.ff80

Image-Auto-Copy is Enabled.

      Stack Port Status                  Neighbors
Unit# Stack-port1       Stack-port2      Stack-port1       Stack-port2
1     dn (1/3/1)        up (1/4/1)       none              U2 (2/3/1)
2     up (2/3/1)        up (2/4/1)       U1 (1/4/1)        U3 (3/3/1)
3     up (3/3/1)        up (3/4/1)       U2 (2/4/1)        U4 (4/3/1)
4     up (4/3/1)        up (4/4/1)       U3 (3/4/1)        U5 (5/3/1)
5     up (5/3/1)        up (5/4/1)       U4 (4/4/1)        U6 (6/3/1)
6     up (6/3/1)        up (6/4/1)       U5 (5/4/1)        U7 (7/3/1)
7     up (7/3/1)        up (7/4/1)       U6 (6/4/1)        U8 (8/3/1)
8     up (8/3/1)        up (8/4/1)       U7 (7/4/1)        U9 (9/3/1)
9     up (9/3/1)        up (9/4/1)       U8 (8/4/1)        U10 (10/3/1)
10    up (10/3/1)       up (10/4/1)      U9 (9/4/1)        U11 (11/3/1)
11    up (11/3/1)       up (11/4/1)      U10 (10/4/1)      U12 (12/3/1)
12    up (12/3/1)       none             U11 (11/4/1)      none

Unit# System uptime
1     17 hours 38 minutes 45 seconds
2     17 hours 38 minutes 43 seconds
3     17 hours 38 minutes 45 seconds
4     17 hours 38 minutes 44 seconds
5     17 hours 38 minutes 44 seconds
6     17 hours 38 minutes 44 seconds
7     17 hours 38 minutes 44 seconds
8     17 hours 38 minutes 45 seconds
9     17 hours 38 minutes 43 seconds
10    17 hours 32 minutes 24 seconds
11    1 minutes 9 seconds
12    1 minutes 9 seconds
ICX7450-24 Route
```

show stack failover

Displays information about stack failover.

Syntax **show stack failover**

Modes Privileged EXEC mode

Usage Guidelines Use the **show stack failover** command to view information about rapid failover for the stack. This command displays if the standby is ready to takeover or not.

Examples The following example shows which unit is the current standby device and its status.

```
device# show stack failover

Current standby is unit 2. state=ready
Standby u2 - protocols ready, can failover
```

show stack flash

Displays information about flash memory for stack members.

Syntax **show stack flash**

Modes Privileged EXEC mode

Usage Guidelines Use the **show stack flash** command to display information about flash memory for stack members.

Command Output The **show stack flash** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
role	Specifies the role of the stack unit. The roles are controller, standby, or member.
priority	Specifies the priority value assigned to the stack unit. The default value is 128.
config	Indicates the port state (up or down) and identifies the port by number (stack-ID/slot/port). A port with the up status of up is connected to the stack, and a ports with the status of down (dn) is not connected to the stack.
The rest of the fields are used for debug purposes only.	

Examples The following example display flash memory information for an ICX 6610.

```
device# show stack flash
There is no startup-config.old
Stack flash that was read in bootup:
ICX6610-48P, ID =4, role= active, pri=200, config=1, jumbo=X PPVLAN=X S2M=0 FIPS=X
stack p: [0]=4/2/1 [1]=4/2/6 default p: 4/2/1(5) 4/2/6(5), , , hash-chain=X vlan#=X
ve#=X stp#=X
active-chg=0
Current written stack flash:
ICX6610-48P, ID =4, role= active, pri=200, config=1, jumbo=X PPVLAN=X S2M=0 FIPS=X
stack p: [0]=4/2/1 [1]=4/2/6 default p: 4/2/1(5) 4/2/6(5), , , hash-chain=X vlan#=X
ve#=X stp#=X
```

show stack link-sync

Displays the status of the link synchronization.

Syntax **show stack link-sync status**

Parameters **status**

Displays link status information.

Modes Privileged EXEC mode

Command Output The **show stack link-sync status** command displays the following information:

Output field	Description
STACKING_LINK_GLOBAL_CTRL messages (sent, received)	Number of global control messages sent and received.
STACKING_LINK_INDIVIDUAL_CTRL messages (sent, received)	Number of individual link control messages sent and received.
STACKING_LINK_STATUS messages (sent, received)	Number of link status control messages sent and received.
STACKING_POE_SCTRL messages (sent, received)	Number of Power over Ethernet (POE) control messages sent and received.
STACKING_POE_STATUS messages (sent, received)	Number of POE status messages sent and received.
global_ctrl_dest	Hexadecimal address of the global control destination.
individual_ctrl_dest	Hexadecimal address of the individual link control destination
status_dest	Number representing the destination status.

Examples The following example shows link synchronization information for an ICX 6610.

```
device# show stack link-sync status
STACKING_LINK_GLOBAL_CTRL messages sent: 0, received: 0
STACKING_LINK_INDIVIDUAL_CTRL messages sent: 359, received: 0
STACKING_LINK_STATUS messages sent: 22300, received: 128883
STACKING_POE_SCTRL messages sent: 0, received: 0
STACKING_POE_STATUS messages sent: 0, received: 0
global_ctrl_dest: ffffffff
individual_ctrl_dest: ee
status_dest: 30
```

show stack neighbors

Displays information about stack member neighbors.

Syntax **show stack neighbors**

Modes Privileged EXEC mode

Usage Guidelines Stack neighbors are identified by unit ID for each stack unit.

Command Output The **show stack neighbors** command displays the following information:

Output field	Description
U#	The identification number of the unit in the stack. Each unit in the stack has a unique identification number.
Stack-port1	Identifies the neighbor stack unit for stack-port1 of the stack unit with this unit identification number (U#). The neighbor stack unit for stack-port1 of each unit in the stack is listed.
Stack-port2	Identifies the neighbor stack unit for stack-port2 of the stack unit with this unit identification number (U#). The neighbor stack unit for stack-port2 of each unit in the stack is listed.

Examples The following example output is for an ICX 6610 device in a stack with seven members.

```
device# show stack neighbors
U#  Stack-port1             Stack-port2
1   unit7 (7/2/1-7/2/5)     unit2 (2/2/6-2/2/10)
2   unit3 (3/2/1-3/2/5)     unit1 (1/2/6-1/2/10)
3   unit2 (2/2/1-2/2/5)     unit4 (4/2/6-4/2/10)
4   unit5 (5/2/1-5/2/5)     unit3 (3/2/6-3/2/10)
5   unit4 (4/2/1-4/2/5)     unit6 (6/2/1-6/2/5)
6   unit5 (5/2/6-5/2/10)    unit7 (7/2/6-7/2/10)
7   unit1 (1/2/1-1/2/5)     unit6 (6/2/6-6/2/10)
Topology: Ring, 7 unit(s), order: 4 3 2 1 7 6 5
    active
    +-+        +-+        +-+        +-+        +-+        +-+
=2/1|4|2/6==2/6|3|2/1==2/1|2|2/6==2/6|1|2/1==2/1|7|2/6==2/6|6|2/1=
|   +-+        +-+        +-+        +-+        +-+        +-+   |
|                                                               |
|                                                          standby|
|                                                           +-+   |
-----------------------------------------------------------2/1|5|2/6=
                                                            +-+
```

show stack rel-ipc stats

Displays statistics on reliable Interprocessor Communications (IPC) communications that occur between stack units during a session.

Syntax **show stack rel-ipc stats** { **unit** *num* }

Parameters

rel-ipc

Abbreviation for reliable Interprocessor Communications, which designates the proprietary packets exchanged between stack units during a communications session.

stats

Session statistics.

unit *num*

Optional parameter used to specify the stack unit number for which session statistics are to be displayed. If you do not specify a stack unit, session statistics are displayed for all units in the stack.

Modes Privileged EXEC mode

Usage Guidelines To display session statistics for a particular stack unit, specify the stack unit using the **unit** *num* parameters.

To display session statistics for all units in the stack, do not specify a stack unit.

Command Output Depending on whether you specify a stack unit, the **show stack rel-ipc stats** command displays reliable IPC statistics for all units in the stack, or for a single unit in the stack. See the example output below.

Examples The following example is reliable IPC statistics for an ICX 6610 stack.

```
device# show stack rel-ipc stats
Reliable IPC statistics:
Global statistics:
Pkts rcvd w/no session: 0
Msgs rcvd w/no handler: 0
Unit statistics:
Unit 2 statistics:
Msgs sent: 41384  Msgs received: 14052, Pkt sends failed: 0
Message types sent:
    [9]=21674,        [10]=19703,       [11]=2,           [13]=5,
Message types received:
    [9]=14016,        [10]=2,           [11]=28,          [13]=6,
Session statistics: base-channel, unit 2, channel 0:
Session state: established (last established 15 hours 33 minutes 31 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14636, Msgs received: 14039
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 30892, Pkts received: 30842
Msg bytes sent: 1828190, Msg bytes received: 1232988
Pkt bytes sent: 2659848, Pkt bytes received: 1763028
Flushes requested: 30, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 888, ACK: 14010, WND: 437, ACK+WND: 0
DAT: 15556, DAT+ACK: 1, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 1069, Zero-window probes sent: 0
Dup ACK pkts rcvd: 1224, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 2, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9899, Pkts received: 10606
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10341308, Pkt bytes received: 127284
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9897, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 49, Zero-window probes sent: 0
Dup ACK pkts rcvd: 757, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 2, channel 3:
Session state: established (last established 15 hours 33 minutes 31 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7011, Msgs received: 4
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7588, Pkts received: 7617
Msg bytes sent: 629316, Msg bytes received: 5840
Pkt bytes sent: 802504, Pkt bytes received: 107508
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 2
DAT: 7584, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 573, Zero-window probes sent: 0
Dup ACK pkts rcvd: 596, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: sync-reliable, unit 2, channel 4:
Session state: established (last established 15 hours 32 minutes 27 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 27, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 53, Pkts received: 40
Msg bytes sent: 39420, Msg bytes received: 1460
Pkt bytes sent: 73836, Pkt bytes received: 1944
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
```

```
Other: 2, ACK: 1, WND: 0, ACK+WND: 0
DAT: 50, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 22, Zero-window probes sent: 0
Dup ACK pkts rcvd: 6, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-2, unit 2, channel 6:
Session state: established (last established 15 hours 33 minutes 30 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 5, Msgs received: 6
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 14, Pkts received: 40
Msg bytes sent: 183, Msg bytes received: 56
Pkt bytes sent: 384, Pkt bytes received: 1052
Flushes requested: 5, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 4, ACK: 5, WND: 0, ACK+WND: 0
DAT: 5, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 0, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Unit 3 statistics:
Msgs sent: 41356  Msgs received: 14007, Pkt sends failed: 0
Message types sent:
    [9]=21623,        [10]=19703,       [11]=29,          [13]=1,
Message types received:
    [9]=14003,        [10]=2,           [13]=2,

Session statistics: base-channel, unit 3, channel 0:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14647, Msgs received: 14003
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 31055, Pkts received: 31403
Msg bytes sent: 1801742, Msg bytes received: 1232204
Pkt bytes sent: 2402644, Pkt bytes received: 1877788
Flushes requested: 32, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1269, ACK: 13911, WND: 437, ACK+WND: 0
DAT: 15346, DAT+ACK: 92, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 966, Zero-window probes sent: 0
Dup ACK pkts rcvd: 661, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 3, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9930, Pkts received: 10599
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10457352, Pkt bytes received: 127200
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9928, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 140, Zero-window probes sent: 0
Dup ACK pkts rcvd: 798, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 3, channel 3:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7004, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7447, Pkts received: 7300
Msg bytes sent: 616352, Msg bytes received: 0
Pkt bytes sent: 774304, Pkt bytes received: 87600
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 0, WND: 0, ACK+WND: 0
DAT: 7445, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 441, Zero-window probes sent: 0
```

```
Dup ACK pkts rcvd: 295, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-3, unit 3, channel 7:
Session state: established (last established 15 hours 33 minutes 48 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 1, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 3, Pkts received: 2
Msg bytes sent: 35, Msg bytes received: 20
Pkt bytes sent: 76, Pkt bytes received: 52
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 1, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 0, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Unit 4 statistics:
Msgs sent: 41337  Msgs received: 14035, Pkt sends failed: 0
Message types sent:
    [9]=21632,        [10]=19702,       [11]=2,           [13]=1,
Message types received:
    [9]=14031,        [10]=2,           [13]=2,
Session statistics: base-channel, unit 4, channel 0:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14630, Msgs received: 14031
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 30186, Pkts received: 31052
Msg bytes sent: 1801548, Msg bytes received: 1234680
Pkt bytes sent: 2325044, Pkt bytes received: 1857824
Flushes requested: 30, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1199, ACK: 13879, WND: 434, ACK+WND: 4
DAT: 14522, DAT+ACK: 148, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 197, Zero-window probes sent: 0
Dup ACK pkts rcvd: 560, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 4, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9852, Pkts received: 10675
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10284896, Pkt bytes received: 128112
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9850, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 2, Zero-window probes sent: 0
Dup ACK pkts rcvd: 826, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 4, channel 3:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7004, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7051, Pkts received: 7240
Msg bytes sent: 616352, Msg bytes received: 0
Pkt bytes sent: 733028, Pkt bytes received: 86880
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 3, ACK: 0, WND: 0, ACK+WND: 0
DAT: 7048, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 44, Zero-window probes sent: 0
Dup ACK pkts rcvd: 234, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-4, unit 4, channel 8:
Session state: established (last established 15 hours 33 minutes 48 seconds ago)
```

```
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 1, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 5, Pkts received: 8
Msg bytes sent: 35, Msg bytes received: 20
Pkt bytes sent: 140, Pkt bytes received: 264
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 1, WND: 0, ACK+WND: 0
DAT: 2, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 1, Zero-window probes sent: 0
Dup ACK pkts rcvd: 1, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
```

The following example displays session statistics for stack unit 3.

```
device# show stack rel-ipc stats unit 3
Unit 3 statistics:
Msgs sent: 1217  Msgs received: 509, Pkt sends failed: 0
Message types sent:
[9]=1182,         [10]=2,           [11]=2,           [13]=2,
[19]=29,
Message types received:
[9]=506,          [10]=1,           [13]=2,
Session statistics, unit 3, channel 0:
Session state: established (last established 32 minutes 19 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 971, Msgs received: 506
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 1205, Pkts received: 1088
Msg bytes sent: 44281, Msg bytes received: 19308
Pkt bytes sent: 238004, Pkt bytes received: 34652
Flushes requested: 59, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 504, WND: 7, ACK+WND: 0
DAT: 691, DAT+ACK: 1, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 129, Zero-window probes sent: 0
Dup ACK pkts rcvd: 18, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 2:
Session state: established (last established 32 minutes 17 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 0, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 1, Pkts received: 7
Msg bytes sent: 0, Msg bytes received: 0
Pkt bytes sent: 12, Pkt bytes received: 84
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 0, WND: 0, ACK+WND: 0
DAT: 0, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 7, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 3:
Session state: established (last established 32 minutes 19 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 242, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 243, Pkts received: 246
Msg bytes sent: 8712, Msg bytes received: 0
Pkt bytes sent: 12596, Pkt bytes received: 2952
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 0, WND: 0, ACK+WND: 0
DAT: 242, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 4, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 6:
Session state: established (last established 32 minutes 17 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 2, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 8, Pkts received: 13
Msg bytes sent: 123, Msg bytes received: 20
Pkt bytes sent: 232, Pkt bytes received: 296
Flushes requested: 2, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 5, ACK: 1, WND: 0, ACK+WND: 0
DAT: 2, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
```

```
Dup ACK pkts rcvd: 6, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
```

show stack resource

Displays resource information for a stack unit.

Syntax **show stack resource**

Modes Privileged EXEC mode

Command Output The **show stack resource** command displays the following information:

Output field	Description
alloc	Memory allocated
in-use	Memory in use
avail	Available memory
get-fail	The number of get requests that have failed
limit	The maximum memory allocation
get-mem	The number of get-memory requests
size	The size
init	The number of requests initiated

Examples The following example displays stack resource statistics for an ICX 6610 stack unit.

```
device# show stack resource

                    alloc in-use avail get-fail   limit get-mem size init
register attribute   4800   2710  2090        0  556800    4810  334 2400
general 12B data       32     10    22        0    7424      12   12   32
RB-tree node         4096   2714  1382        0  237568    3026   18 1024
variable length link 3905      4  3901        0  905960       4    8 3905
AU msg dev0          4092      0  4092        0   16368       0   16 4092
AU msg dev1          4092      0  4092        0   16368       0   16 4092
```

show stack stack-ports

Displays status information about stack-ports.

Syntax **show stack stack-ports**

Modes Privileged EXEC mode

Global configuration mode

Command Output For ICX devices, an equal sign is used to indicate connections between trunk ports and the up port status is listed for all trunked ports. The **show stack stack-ports** command displays the following information:

Output field	Description
U# or ID	Stack unit identification number.
Stack-port 1	Indicates port status (up or down) and identifies the port by number (stack-ID/slot/port).
Stack-port 2	Indicates port status (up or down) and identifies the port by number (stack-ID/slot/port).
Stack-ID up (stack-ID/slot/port)	Indicates status (up or down) for the stack unit and the status (up or down) of all configured stacking ports on the unit by number (stack-ID/slot/port).

Examples The following output is for an FCX stack with five stacking units.

```
device(config)# show stack stack-ports
ID      Stack-port1      Stack-port2
1       up   (1/2/1)     up   (1/2/2)
2       up   (2/2/1)     up   (2/2/2)
3       up   (3/2/1)     up   (3/3/1)
4       up   (4/2/1)     up   (4/3/1)
5       up   (5/2/1)     up   (5/3/1)
```

The following output is for an ICX 6610 in a seven-unit stack configured in a ring topology.

```
device# show stack stack-ports
    active
    +-+        +-+        +-+        +-+        +-+        +-+
=2/1|4|2/6==2/6|3|2/1==2/1|2|2/6==2/6|1|2/1==2/1|7|2/6==2/6|6|2/1=
|   +-+        +-+        +-+        +-+        +-+        +-+   |
|                                                               |
|                                                            standby|
|                                                             +-+   |
-------------------------------------------------------------2/1|5|2/6=
                                                              +-+

U#  Stack-port1                                    Stack-port2
1   up (1/2/1-1/2/5)                               up (1/2/6-1/2/10)
    up ports: 1/2/1, 1/2/2, 1/2/3, 1/2/4, 1/2/5
    up ports: 1/2/6, 1/2/7, 1/2/8, 1/2/9, 1/2/10
2   up (2/2/1-2/2/5)                               up (2/2/6-2/2/10)
    up ports: 2/2/1, 2/2/2, 2/2/3, 2/2/4, 2/2/5
    up ports: 2/2/6, 2/2/7, 2/2/8, 2/2/9, 2/2/10
3   up (3/2/1-3/2/5)                               up (3/2/6-3/2/10)
    up ports: 3/2/1, 3/2/2, 3/2/3, 3/2/4, 3/2/5
    up ports: 3/2/6, 3/2/7, 3/2/8, 3/2/9, 3/2/10
4   up (4/2/1-4/2/5)                               up (4/2/6-4/2/10)
    up ports: 4/2/1, 4/2/2, 4/2/3, 4/2/4, 4/2/5
    up ports: 4/2/6, 4/2/7, 4/2/8, 4/2/9, 4/2/10
5   up (5/2/1-5/2/5)                               up (5/2/6-5/2/10)
    up ports: 5/2/1, 5/2/2, 5/2/3, 5/2/4, 5/2/5
    up ports: 5/2/6, 5/2/7, 5/2/8, 5/2/9, 5/2/10
6   up (6/2/1-6/2/5)                               up (6/2/6-6/2/10)
    up ports: 6/2/1, 6/2/2, 6/2/3, 6/2/4, 6/2/5
    up ports: 6/2/6, 6/2/7, 6/2/8, 6/2/9, 6/2/10
7   up (7/2/1-7/2/5)                               up (7/2/6-7/2/10)
    up ports: 7/2/1, 7/2/2, 7/2/3, 7/2/4, 7/2/5
    up ports: 7/2/6, 7/2/7, 7/2/8, 7/2/9, 7/2/10
```

show statistics l2-tunnel

Displays Layer 2 tunnel statistics such as the status of the tunnel and packet flow.

Syntax **show statistics l2-tunnel** *tunnel-id*

Parameters *tunnel-id*

Specifies the tunnel ID for the Layer 2 tunnel interface.

Modes Privileged EXEC mode

Global configuration mode

Command Output The **show statistics l2-tunnel** command displays the following information.

Output field	Description
Type	VXLAN tunnels
Tunnel Status	Status of the tunnel
Packet Received / Packet Sent	Statistics of the packet flow
KA received / KA sent	Statistics of Keepalive (Currently not supported)

Examples The following example shows the output of the **show statistics l2-tunnel** command:

```
device# show statistics l2-tunnel
L2 Tunnels
  Type     Tunnel Status  Packet Received  Packet Sent  KA recv  KA sent
  VXLAN1   down/down       0                0            0        0
  VXLAN2   up/up           0                0            0        0
```

History

Release version	Command history
8.0.10d	This command was introduced.

show statistics stack-ports

Displays information about all stacking ports in a stack topology.

Syntax **show statistics stack-ports**

Modes Privileged EXEC mode

Command Output The **show statistics stack-ports** command displays the following information:

Output field	Description
Port	The number of the port (stack-unit number, slot number, and port number).
In Packets	The number of packets received on this port (incoming packets).
Out Packets	The number of packets sent from this port (outgoing packets).
In Errors	The number of errors received on this port (incoming errors).
Out Errors	The number of errors sent from this port (outgoing errors).

Examples The following example output is statistics for all stack ports in a stack with seven member units.

```
device# show statistics stack-ports

Port     In Packets   Out Packets   In Errors   Out Errors
1/2/1         22223          4528           0            0
1/2/2         35506          3844           0            0
2/2/1          3161         34173           0            0
2/2/2         24721          3676           0            0
3/2/1          3048         23881           0            0
3/2/2         13540          2857           0            0
4/2/1          2862         13537           0            0
4/2/2          3626          3184           0            0
5/2/1          3183          3621           0            0
5/2/2          3265         13508           0            0
6/2/1         14020          3655           0            0
6/3/1          3652         17705           0            0
7/2/1         17705          3658           0            0
7/3/1          4047         21802           0            0
TOTAL        154559        153629           0            0
```

Commands Sn - Z

snmp-server enable traps mac-notification

Enables the MAC-notification trap whenever a MAC address event is generated on a device or an interface.

Syntax **snmp-server enable traps mac-notification**

no snmp-server enable traps mac-notification

Command Default MAC-notification traps are disabled on the device.

Modes Global configuration

Interface configuration

Usage Guidelines The **no** form of this command disables SNMP traps for MAC-notification events. The SNMP MAC-notification trap functionality allows an SNMPv3 trap to be sent to the SNMP manager when MAC addresses are added or deleted in the device.

Examples The following example enables SNMP traps on the device for MAC-notification globally:

```
device(config)# snmp-server enable traps mac-notification
```

The following example disables SNMP traps on the device for MAC-notification globally:

```
device(config)# no snmp-server enable traps mac-notification
```

History

Release version	Command history
08.0.10	This command was introduced.

snmp-server group

Creates user-defined groups for SNMPv1/v2c/v3 and configures read, write, and notify permissions to access the MIB view.

Syntax **snmp-server group** *groupname* { **v1** | **v2c** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

no snmp-server group *groupname* { **v1** | **v2c** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

snmp-server group *groupname* **v3** { **auth** | **noauth** | **priv** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

no snmp-server group *groupname* **v3** { **auth** | **noauth** | **priv** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *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.

NOTE
This command is not used for SNMP version 1 and SNMP version 2. In these versions, groups and group views are created internally using community strings. When a community string is created, two groups are created, based on the community string name. One group is for SNMP version 1 packets, while the other is for SNMP version 2 packets.

Parameters

groupname
Specifies the name of the SNMP group to be created.

v1
Specifies SNMP version 1.

v2c
Specifies SNMP version 2.

v3
Specifies SNMP version 3.

auth
Specifies that only authenticated packets with no privacy are allowed to access the specified view. This parameter is available only for SNMPv3 user groups.

noauth
Specifies that no authentication and no privacy are required to access the specified view. This parameter is available only for SNMPv3 user groups.

priv
Specifies that authentication and privacy are required from the users to access the view. This parameter is available only for SNMPv3 user groups.

access
Specifies an access list associated with the SNMP group.

standard-ACL-id
Specifies the standard IP access list and allows the incoming SNMP packets to be filtered based on the standard ACL attached to the group.

ipv6
Specifies the IPv6 ACL for the SNMP group.

ipv6-ACL-name

Specifies the IPv6 access list and allows incoming SNMP packets to be filtered based on the IPv6 ACL attached to the group.

notify *viewname*

Specifies the name of the view that enables you to provide access to the MIB for trap or inform. This allows the administrators to restrict the scope of varbind objects that will be part of the notification. All of the varbinds need to be in the included view for the notification to be created.

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.

viewname

Specifies the name of the view to which the SNMP group members have access. If no view is specified, then the group has no access to the MIB. The default viewname is "all", which allows access to the entire MIB.

Modes

Global configuration mode

Usage Guidelines

Maximum number of SNMP groups supported is 10.

The **no** form of the command removes the configured SNMP server group.

Examples

The following example creates SNMP server group entries for SNMPv3 user group with auth permission.

```
device(config)# snmp-server group admin v3 auth ipv6 acl_1 read all write all notify
all
```

History

Release version	Command history
08.0.20a	The **ipv6** *ipv6-ACL-name* keyword-argument pair was introduced.

spanning-tree designated-protect

Disallows the designated forwarding state on a port in STP 802.1d or 802.1w.

Syntax **spanning-tree designated-protect**

no spanning-tree designated-protect

Command Default STP (802.1d or 802.1w) can put a port into designated forwarding state.

Modes Interface configuration mode

Usage Guidelines The **no** form of this command allows the designated forwarding state on a port in STP 802.1d or 802.1w. If STP tries to put a port into designated forwarding state, the device puts this port into the designated inconsistent STP state. This is effectively equivalent to the listening state in STP in which a port cannot forward any user traffic. When STP no longer marks this port as a designated port, the port is automatically removed from the designated inconsistent state.

NOTE
You use this command to enable Designated Protection at the port-level while the designated inconsistent state is a per-STP-instance, per-port state.

NOTE
You cannot enable Designated Protection and Root Guard on the same port.

Examples The following example disallows the designated forwarding state on interface 1/1/1.

```
device(config)# ethernet interface 1/1/1
device(config-if-e1000-1/1/1)# spanning-tree designated-protect
```

History

Release version	Command history
07.3.00g	This command was introduced.

stack disable

Prevents a device from joining a traditional stack and from listening for, or sending, stacking packets.

Syntax **stack disable**

no stack disable

Command Default Stacking is disabled by default.

Modes Global configuration mode and Stack unit configuration mode

Usage Guidelines To remove the restriction that prevents the unit from joining a stack, use the **no stack disable** command.

Examples The following example disables the device from joining a stack.

```
device# configure terminal
device(config)# stack disable
Disable stacking. This unit will not be a part of any stack
```

History

Release version	Command history
08.0.00a	This command was introduced.

stack enable

Enables stack configuration on the device. Enter this command on the intended active controller.

Syntax **stack enable**

no stack enable

Command Default Stacking is not enabled on the device.

Modes Global configuration mode

Stack unit configuration mode

Usage Guidelines Use the **no** form of the command to remove stacking capability from the device.

NOTE

When you use the **no stack enable** command, the unit can still be called to join an active stack. To prevent this, use the **stack disable** command instead.

You must remove all configuration information from the port before issuing the **stack enable** command.

For manual configuration, the **stack enable** command must be issued on each device in the stack.

Examples The following example enables stack configuration on the device.

```
device# config terminal
device(config)# stack enable
Enable stacking. This unit actively participates in stacking
```

History

Release version	Command history
08.0.00a	This command was introduced.

stack mac

Manually configures a specific MAC address for a traditional stack.

Syntax **stack mac** *mac-address*

no stack mac *mac-address*

Command Default Beginning with FastIron release 08.0.20, when a stack is enabled or when hitless-failover occurs, a default stack MAC address is assigned if none is configured. In earlier releases, the stack assumed the MAC address of the active controller by default.

Parameters *mac-address*

Specifies the MAC address to be used for the stack.

Modes Active stack controller configuration mode

Usage Guidelines Enter the **no** form of this command to revert to the use of the active controllers' MAC address.

The MAC address is a hexadecimal value entered in the format xxxx.xxxx.xxxx.

Examples The following example configures the stack MAC address manually as 0000.0000.0011.

```
device(config)# stack mac 0000.0000.0011
device(config)# show running-config
Current configuration:
!
ver 05.0.01 100T7e1
!
stack 1
module 1 fcx-48-port-copper-base-module
module 2 fcx-cx4-1-port-10g-module
priority 80
stack 2
module 1 fcx-24-port-copper-base-module
module 2 fcx-cx4-1-port-10g-module
module 3 fcx-cx4-1-port-10g-module
stack enable
stack mac 0000.0000.0011
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Stack behavior was modified so that a default MAC address is assigned when the stack is enabled or when hitless failover occurs if no stack MAC address has been configured.

stack-port

Selects only one of the two stacking ports as a stacking port, which allows you to use the other port as a data port.

Syntax **stack-port** *unit*/*slot*/*port*

no stack-port

Command Default By default, both default ports serve as stacking ports on an FCX or ICX stack unit.

Parameters *unit*

Stack unit ID

slot

Slot or module on the unit where the interface resides.

port

Interface to be configured as the sole stack port on the unit.

Modes Stack-unit configuration mode.

Usage Guidelines The **no** form of the command restores both default stacking ports on the device.

The **stack-port** command should not be used on a live stack.

Examples The following example configures Port 3/2/1 as the only stacking port on stack unit 3.

```
device# configure terminal
device(config)# stack unit 3
device(config-unit-3)# stack-port 3/2/1
Set only one stacking port 3/2/1
```

stack secure-setup

Configures a stack automatically, to add units to an existing traditional stack, or to change stack member IDs.

Syntax **stack secure-setup**

Modes Privileged EXEC mode of a stack unit

Usage Guidelines Stacking must be enabled with the **stack enable** command before the **stack secure-setup** command can be issued.

When the **stack secure-setup** command is issued on a unit that is not already the active controller, the unit becomes the active controller.

Examples In the following example, an FCX traditional stack is formed using **stack secure-setup**.

```
device# stack secure-setup
device# Discovering the stack topology...
Current Discovered Topology - RING
Available UPSTREAM units
Hop(s) Type MAC Address
1 FCX624 0000.0039.2d40
2 FCX624 0000.00d5.2100
Available DOWNSTREAM units
Hop(s) Type MAC Address
1 FCX624 0000.00d5.2100
2 FCX624 0000.0039.2d40
Do you accept the topology (RING) (y/n)?: y
Selected Topology:
Active Id Type MAC Address
1 FCX648 0000.00ab.cd00
Selected UPSTREAM units
Hop(s) Id Type MAC Address
1 3 FCX624 0000.0039.2d40
2 2 FCX624 0000.00d5.2100
Selected DOWNSTREAM units
Hop(s) Id Type MAC Address
1 2 FCX624 0000.00d5.2100
2 3 FCX624 0000.0039.2d40
Do you accept the unit ids (y/n)?: y
```

stack stack-port-resiliency

Configures different levels of corrective steps that an active controller can take to fix stacking ports that cannot send or receive packets, despite the ports being logically operational.

Syntax **stack stack-port-resiliency** *level*

no stack stack-port-resiliency *level*

Command Default The stack-port-resiliency feature is enabled with the *level* variable value set to 1.

Parameters *level*

The value determines the corrective steps that an active controller can take when a stack port is malfunctioning. Then value can range from 0 through 3.

Modes Global configuration mode

Usage Guidelines The **no** form of the **stack stack-port-resiliency** command sets the *level* variable value to 1.

The **stack stack-port-resiliency** command is only supported on an ICX 6610 in a stack.

The corrective steps that can be taken depend on the value of the *level* variable and involve error-disabling malfunctioning ports or reloading one or more stack units. Traffic may be disrupted for a few seconds or longer while the port malfunction is detected and fixed.

If the *level* value is set to 1 and the unit with the malfunctioning port is not an active controller:

- The active controller checks whether other ports in the same static LAG are fully operational.
- If the total bandwidth of the operational static LAG is greater than or equal to 20 Gbps, the malfunctioning port is error-disabled.
- If the total bandwidth of the operational static LAG is less than 20 Gbps and error-disabling all ports of the LAG could disconnect one or more other units from the stack, the unit reloads.
- If the total bandwidth of the operational static LAG is less than 20 Gbps and error-disabling all ports of the LAG would not disconnect any other units from the stack, all the ports of the LAG are error-disabled.

If the *level* value is set to 2 and the unit with the malfunctioning port is not the active controller, the unit reloads. After the reload, if any other non-active controller unit is not able to communicate with the active controller, it also reloads.

If the *level* value is set to 3, the corrective steps in level 2 are performed. If the port is still not operating correctly, the entire stack reloads.

If you use the command and set the *level* variable value to 1, this configuration shows in the **show run** command output. If you use the **no** form of the command, the *level* variable value is set to 1, but the value does not show in the **show run** command output.

NOTE
You can use the **show errdisable summary** command to view a list of all error-disabled ports, along with the reason the ports were error-disabled.

Examples The following example shows the configuration of stack port resiliency on a stack with the *level* variable value set to 2.

```
Device# configure terminal
Device(config)# stack stack-port-resiliency 2
```

History

Release version	Command history
07.3.00g	This command was introduced.

stack suggested-id

Specifies the preferred stack unit ID for a standalone device before it joins a stack.

Syntax **stack suggested-id** *stack-unit*

no stack suggested-id *stack-unit*

Parameters *stack-unit*

Specifies the numeric stack unit ID.

Modes Global configuration mode

Usage Guidelines The **no** form of this command removes the stack unit ID.

The **stack suggested-id** command is configured on a standalone device before it joins a stack and becomes a member. The command is not for the active controller. Because the active controller always keeps its bootup ID during stack formation, it does not use the suggested-id value.

The system attempts to assign a bootup ID of a device as its stack unit ID. However, due to timing issues or the possible unavailability of the bootup ID, a device might not get the stack unit ID that you want when the stack is formed. The optional **stack suggested-id** command allows you to specify the stack unit ID for member devices when you are configuring a traditional or mixed stack using the manual configuration method.

Examples The following example sets the stack unit ID on a standalone device to 3.

```
device# configure terminal
device(config)# stack suggested-id 3
```

stack suppress-warning

Stops periodic output of background stack diagnostic reports.

Syntax **stack suppress-warning**

no stack suppress-warning

Command Default By default, background diagnostics are displayed periodically on the active stack controller.

Modes Stack active controller configuration mode

Usage Guidelines Use the **no** form of the command to restore periodic output of background diagnostic reports.

Examples In the following example, background diagnostic reports are turned off for the stack.

```
Device# configure terminal
Device(config)# stack suppress-warning
```

stack switch-over

Switches active controllers without reloading the stack and without packet loss to services and protocols supported by hitless stacking.

Syntax **stack switch-over**

Command Default With FastIron release 08.0.20, the **stack switch-over** command is allowed by default. In earlier releases, hitless failover must first be enabled.

Modes Global configuration mode on a stack controller

Usage Guidelines Use the **stack switch-over** command before reloading or performing maintenance on the currently active controller. Hitless failover must be enabled for the command to be used; otherwise, an error message is issued.

The command cannot be used during stack election or during configuration of a multi-stack-trunk.

A standby controller must exist and must have learned stack protocols for the command to be used. The standby controller must have the same priority as the active controller for the command to be used.

More than 120 seconds must have passed since the previous switchover or failover for the command to be accepted.

Examples The following example shows the **stack switch-over** command being entered and the resulting output. You must confirm the switch-over before it can take effect by entering **y** when prompted.

```
device# stack switch-over
Standby unit 8 will become active controller, and unit 1 will become standby
Are you sure? (enter 'y' or 'n'): y
Unit 1 is no longer the active controller
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Hitless failover is enabled by default. The **stack switch-over** command is allowed by default as a result.

stack-trunk

Configures a stack to form a trunk from contiguous links on one side of a stack connection.

Syntax **stack-trunk** *stack-unit*/*slotnum*/*portnum* **to** *stack-unit*/*slotnum*/*portnum*

no stack-trunk *stack-unit*/*slotnum*/*portnum* **to** *stack-unit*/*slotnum*/*portnum*

Parameters *stack-unit*

Specifies the stack unit ID.

slotnum

Specifies the slot number.

portnum

Specifies the port number in the slot.

Modes Stack unit configuration mode

Usage Guidelines Use the **no** form of the command to disable the stack trunk configuration.

The **stack-trunk** command must be configured on the stack units on both ends of the trunk. Use this command in a new environment on the first deployment of a stack.

To enable the **stack-trunk** command, the primary port in the trunk must be configured under the **stack-port** command configuration.

Do not use the **stack-trunk** command in a production environment. Use the **multi-stack-trunk** command instead.

Examples In the following example, ports 1/2/3 and 1/2/4 are configured as a stacking trunk on stack unit 1.

```
Device# configure terminal
Device(config)# stack unit 1
Device(config-unit-1)# stack-trunk 1/2/3 to 1/2/4
```

stack unconfigure

Returns a stack member to its pre-stacking configuration or state.

Syntax **stack unconfigure** [**stack-unit** | **all** | **me** | **clean** | **mixed-stack**]

Parameters *stack-unit*

Specifies the numerical ID of a stack member. This option is available on the active controller only.

all

Specifies all stack members. This option is available on the active controller only.

me

Specifies the stack member from which the command is executed. The command removes the unit from the stack and boots it up as a standalone. When the unit rejoins the stack, its standalone startup-config file is saved in a backup file. This option is available on stack member consoles only.

clean

Specifies that the startup configuration be removed from the unit on which the command is executed and that the unit be rebooted as a clean unit. This option is available on stack member consoles only.

mixed-stack

Specifies removal of all peripheral ports and peripheral trunks from ICX 6610 devices. It also specifies recovery and reload of prior ICX 6450 peripheral device configurations, from before the ICX 6450 units were members of the mixed stack. This option is available only on the active controller in a mixed stack.

Modes Privileged EXEC mode

Usage Guidelines When a stack unit that did not have an original startup configuration file is unconfigured, it becomes a clean unit. It is possible that this unit could automatically rejoin the stack if its module configuration matches the configuration of the active controller. To prevent this from happening accidentally, disconnect the unit to be unconfigured, and then issue the **stack unconfigure me** command on it.

Examples **Traditional stack example**

In the following example, stack unit 2 is unconfigured in a traditional stack.

```
Device(config)# show stack
alone: standalone, D: dynamic config, S: static config
ID  Typ    Role    Mac Address    Pri State  Comment
1 S FCX624 active  0012.f2eb.a900 128 local  Ready
2 S FCX648 standby 00f0.424f.4243 0   remote Ready
3 S FCX624 member  00e0.5201.0100 0   remote Ready

Device# stack unconfigure 2
Will recover pre-stacking startup config of this unit, and reset it. Are you sure?
(enter 'y' or 'n'): y

Stack 2 deletes stack bootup flash and recover startup-config.txt from .old

Device# show stack
alone: standalone, D: dynamic config, S: static config
ID  Type   Role    Mac Address    Pri State   Comment
1 S FCX624 active  0012.f2eb.a900 128 local   Ready
2 S FCX648 member  0000.0000.0000 0   reserved
3 S FCX624 standby 00e0.5201.0100 0   remote  Ready
```

Mixed stack example

In the following example, ICX 6450 peripheral devices are removed from a mixed stack. The mixed stack contains two ICX 6610 devices in a ring configuration in the backbone. There are two sub-stacks of three ICX 6450 devices each in the mixed stack.

The following **show stack** output shows the configuration of the mixed stack before the stack **unconfigure mixed-stack** command is executed. The **show stack** command is executed on the active controller.

```
Brocade(config)# show stack
alone: standalone, D: dynamic config, S: static config
ID  Typ    Role    Mac Address    Pri State  Comment
1 S FCX624 active  0012.f2eb.a900 128 local  Ready
2 S FCX648 standby 00f0.424f.4243 0   remote Ready
3 S FCX624 member  00e0.5201.0100 0   remote Ready

Brocade# stack unconfigure 2
Will recover pre-stacking startup config of this unit, and reset it. Are you sure?
(enter 'y' or 'n'): y

Stack 2 deletes stack bootup flash and recover startup-config.txt from .old

Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID  Type   Role    Mac Address    Pri State   Comment
1 S FCX624 active  0012.f2eb.a900 128 local   Ready
2 S FCX648 member  0000.0000.0000 0   reserved
3 S FCX624 standby 00e0.5201.0100 0   remote  Ready

    active       standby
     +---+        +---+
 =2/6| 1 |2/1==2/6| 2 |2/1=
 |   +---+        +---+   |
 |                        |
 |------------------------|

    active                                              standby
      ---         +---+        +---+        +---+        ---
     ( 1 )3/7--2/1| 6 |2/3==2/1| 7 |2/3==2/1| 8 |2/3==3/7( 2 )
      ---         +---+        +---+        +---+         ---

    standby                                             active
      ---         +---+        +---+        +---+         ---
     ( 2 )3/1==2/1| 5 |2/3==2/1| 4 |2/3==2/1| 3 |2/3--3/1( 1 )
      ---         +---+        +---+        +---+         ---
```

The following sequence shows the **stack unconfigure mixed-stack** command being executed on the active controller. After confirmation, all peripheral ports and peripheral trunks are removed from the ICX 6610 units. The peripheral ICX 6450 devices recover their configurations from before they were members of the mixed stack, and they are reloaded.

```
Brocade# stack unconfigure mixed-stack
All the peri-ports/trunks will be removed and all the ICX6450 units will recover
pre-mixed-stacking configuration. Are you sure? (enter 'y' or 'n'): y
Removed peri-ports from configuration:  1/3/1 1/3/7
Removed peri-trunks from configuration: 2/3/1-to-2/3/2 2/3/7-to-2/3/8
```

The **show stack** command is executed on the active controller. The output shows that the ICX 6450 devices are no longer part of the mixed stack because the MAC addresses are all zeroes, the State column shows “reserve,” and the device status in the Comment column does not show “Ready.”

The Role column still shows “member” because the active controller holds the configuration of the former stack member in reserve so that it can form a stack later if a stack is merged or formed.

```
Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6610-24F  active  748e.f891.c5b8 128 local   Ready
2  S ICX6610-48P  standby 748e.f834.4d14   0 remote  Ready
3  S ICX6450-24   member  0000.0000.0000   0 reserve
```

```
4  S ICX6450-24P  member  0000.0000.0000   0 reserve
5  S ICX6450-24P  member  0000.0000.0000   0 reserve
6  S ICX6450-48   member  0000.0000.0000   0 reserve
7  S ICX6450-48   member  0000.0000.0000   0 reserve
8  S ICX6450-24P  member  0000.0000.0000   0 reserve

    active       standby
      +---+        +---+
 =2/6| 1 |2/1==2/6| 2 |2/1=
  |   +---+        +---+   |
  |                        |
  |------------------------|
```

Use the **show stack** command to verify that peripheral devices, such as ICX 6450 devices, are no longer part of the mixed stack.

In the following example, the Role column shows “alone,” which indicates a standalone device. This means that the device was a standalone device before joining the mixed stack.

```
Brocade# show stack

***** Warning! stack is not enabled. *****

alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6450-24P  alone   748e.f8b0.6c00   0 local   None:0


     +---+
  2/1| 1 |2/3
     +---+
Current stack management MAC is 748e.f8b0.6c00
Note: no "stack mac" config. My MAC will change after failover.
```

In the following example, the Role column shows “active,” “standby,” or “member,” which indicates that these devices are part of a stack. This means that the devices were part of a traditional stack before joining the mixed stack.

```
Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6450-24P  active  748e.f8b0.6c00 128 local   Ready
2  S ICX6450-48   standby 748e.f8d4.2300   0 remote  Ready
3  S ICX6450-48   member  748e.f8d4.02c0   0 remote  Ready

                 standby      active
     +---+        +---+        +---+
  2/1| 3 |2/3--2/1| 2 |2/3--2/1| 1 |2/3
     +---+        +---+        +---+
Standby u2 - No hitless failover. Reason: hitless-failover not configured
Current stack management MAC is 748e.f8b0.6c00
Note: no "stack mac" config. My MAC will change after failover.
```

History

Release	Command History
07.4.00	This command was introduced.
08.0.00a	The **mixed-stack** option was added. The **rollback** option was deprecated.

store-and-forward

Resets the switching method for forwarding packets from cut-through to store-and-forward.

Syntax **store-and-forward**

no store-and-forward

Command Default The switching method is cut-through.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default packet-forwarding method to cut-through.

Ethernet devices support two basic switching methods for packet forwarding: store-and-forward and cut-through. The default method on ICX 7750 devices is cut-through. You can configure the **store-and forward** command to change it to store-and-forward.

NOTE
You must save the configuration and reload for the change to take effect.

A store-and-forward device does not make a forwarding decision on a data packet until it has received the whole frame and checked its integrity; a cut-through device starts the forwarding process soon after it makes the forwarding decision on an incoming frame that is, it might start forwarding before the entire packet is received. This reduces forwarding latency, especially for longer packets. However, there are many factors to consider when selecting which switching method is best for your environment and in some cases it is desirable to change from the default method and configure a device to store-and-forward.

The following table describes some of the differences in how packets are handled depending on the switching method.

Feature	Cut-through	Store-and-forward
Forwarding	Data forwarding starts before an entire packet is received	Device waits for entire packet received before processing.
Latency	Low latency, less than 1 micro second.	Higher latency; latency depends on frame size.
FCS Errors	FCS errors may be propagated from one device to another.	FCS errors are checked and error packets are discarded in the MAC receive.
MTU size	MTU size is validated by MAC receive. Oversize packets are marked as error packets but not dropped in the MAC receive.	MTU size is validated by MAC receive. Oversize packets are dropped at the MAC layer.

Examples This example globally enables **store-and-forward** packet switching and saves the configuration.

```
Device(config)# store-and-forward
Device(config)# write memory
Device(config)# end
```

History

Release version	Command history
08.0.10b	This command was introduced.

symmetrical-flow-control enable

Enables symmetrical flow control (SFC) globally for priorities.

Syntax **symmetrical-flow-control enable** [**all**]

no symmetrical-flow-control enable

Command Default SFC is globally disabled.

Parameters **all**

Specifies SFC on all priorities. If you do not specify the **all** keyword, SFC is enabled only on priorities 0-4. This parameter is optional.

Modes Global configuration mode

Usage Guidelines The **no** form of this restores the default flow-control settings.

Configuring the **symmetrical-flow-control enable** command enables SFC globally for priorities 0-4 by default and optionally for all priorities (0-7)

By default, the system runs in tail-drop mode, with all ports honoring 802.3x flow control and disabling 802.3x transmit. The **symmetrical-flow-control enable** command enables transmission of 802.3x pause frames.

Configuring the **symmetrical-flow-control enable** command changes priority-to-PG mapping.

You cannot configure the **symmetrical-flow-control enable** command if the **priority-flow-control** command is enabled.

If the **symmetrical-flow-control enable** command is not enabled, you cannot configure the **flow-control generate-only** or the **flow-control both** commands in interface configuration mode.

NOTE
In FastIron Release 08.0.20 and later releases, SFC is not supported for ports across stack units in ICX 7750 devices or across stack units or for ports across master and slave packet-processor (pp) devices in ICX7450-48 units.

Examples The following example shows how to enable SFC:

```
Device(config)# symmetrical-flow-control enable
```

The following example shows how to enable all priorities to send the IEEE 802.3x pause:

```
Device(config)# symmetrical-flow-control enable all
```

The following example shows how to enable SFC for Generate-only mode:

```
Device(config)# symmetrical-flow-control enable
Device(config)# flow-control generate-only
```

The following example shows how to enable SFC for both Honor and Generate-only mode:

```
Device(config)# symmetrical-flow-control enable
Device(config)# flow-control both
```

History

Release version	Command history
8.0.10	This command was introduced.

system-max igmp-snoop-group-addr

Sets the maximum number of IGMP group addresses on a device.

Syntax **system-max igmp-snoop-group-addr** *num*

no system-max igmp-snoop-group-addr

Command Default The default number of IGMP group addresses is supported.

Parameters *num*

Specifies the maximum number of IGMP group addresses supported. The range is a value from 256 through 8192. The default for IGMP snooping group addresses is 4096, except for ICX 6430 devices where the default is 1024.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default maximum.

The configured number of IGMP group addresses is the upper limit of an expandable database. Client memberships exceeding the group limit are not processed.

The following describes the IGMP group address limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 IGMP group addresses.
- ICX 6430 devices support up to 4096 IGMP group addresses.
- ICX 6650 devices support 8192 IGMP group addresses.
- ICX 7750 switches support 8192 IGMP group addresses.
- ICX 7750 routers support 6K IGMP group addresses.

Examples This example shows how to set maximum number of IGMP snooping group addresses to 1600.

```
Device(config)#system-max igmp-snoop-group-addr 1600
```

system-max igmp-snoop-mcache

Configures the maximum number of IGMP snooping cache entries supported on a device.

Syntax **system-max igmp-snoop-mcache** *num*

no system-max igmp-snoop-mcache

Command Default The default number of IGMP snooping cache entries is supported.

Parameters *num*

Specifies the maximum number of IGMP snooping cache entries supported. The range is a value from 256 through 8192. The default is 512 entries except on ICX 6430 devices, where the default is 256.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default maximum.

The following describes the IGMP snooping multicast cache (mcache) resource limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 IGMP snooping mcache entries.
- ICX 6430 devices support up to 2048 IGMP snooping mcache entries.
- ICX 6650 devices support 8192 IGMP snooping mcache entries.
- ICX 7750 switches support 8192 IGMP snooping mcache entries.
- ICX 7750 routers support 6K IGMP snooping mcache entries.

Examples This example shows how to configure the maximum number of IGMP snooping mcache entries supported on the device to 2000.

```
Device(config)#system-max igmp-snoop-mcache 2000
```

system-max mac-notification-buffer

Changes the value of the MAC-notification buffer.

Syntax **system-max mac-notification-buffer** *size*

no system-max mac-notification-buffer *size*

Command Default The default buffer size is 4000.

Parameters ***size***

Sets the buffer queue size to maintain MAC-notification events.

Modes Global configuration

Usage Guidelines

Examples This example changes the value of the MAC-notification buffer:

```
device(config)# system-max mac-notification-buffer 8000
```

This example sets the MAC-notification buffer to default size:

```
device(config)# no system-max mac-notification-buffer 4000
```

History

Release version	Command history
08.0.10	This command was introduced.

system-max mld-snoop-group-addr

Sets the maximum number of multicast listening discovery (MLD) group addresses on a device.

Syntax **system-max mld-snoop-group-addr** *num*

no system-max mld-snoop-group-addr

Command Default The default number of MLD group addresses is supported.

Parameters *num*

Specifies the maximum number of MLD group addresses supported. The range is a value from 256 through 8192. The default for MLD snooping group addresses is 4096, except for ICX 6430 devices where the default is 1024.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default maximum.

The configured number of MLD group addresses is the upper limit of an expandable database. Client memberships exceeding the group limit are not processed.

The following describes the MLD group address limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 MLD group addresses.
- ICX 6430 devices support up to 4096 MLD group addresses.
- ICX 6650 devices support 8192 MLD group addresses.
- ICX 7750 switches support 8192 MLD group addresses.
- ICX 7750 routers support 6K MLD group addresses.

Examples This example shows how to set maximum number of MLD snooping group addresses to 4000.

```
Device(config)#system-max mld-snoop-group-addr 4000
```

system-max mld-snoop-mcache

Configures the maximum number of multicast listening discovery (MLD) snooping cache entries supported on a device.

Syntax **system-max mld-snoop-mcache** *num*

no system-max mld-snoop-mcache

Command Default The default number of MLD snooping cache entries is supported.

Parameters *num*

Specifies the maximum number of MLD snooping cache entries supported. The range is 256 to 8192. The default is 512 entries except on ICX 6430 devices, where the default is 256.

Modes Global configuration mode

Usage Guidelines The **no** form of this command restores the default maximum.

The following describes the MLD snooping multicast cache (mcache) resource limits for Brocade devices:

- FCX, FSX, ICX 6610, ICX 6450 and ICX 6650 devices support up to 8192 MLD snooping mcache entries.
- ICX 6430 devices support up to 2048 MLD snooping mcache entries.
- ICX 7750 routers support 3072 MLD snooping mcache entries; ICX 7750 switches support 8192 MLD snooping mcache entries.
- In Release 8.0.10a and later releases, ICX 7750 routers support 6144 MLD snooping mcache entries; ICX 7750 switches support 8192 MLD snooping mcache entries.

Examples This example shows how to set the maximum number of MLD snooping mcache entries to 8000.

```
Device(config)#system-max mld-snoop-mcache 8000
```

traffic-policy count

Configures a traffic policy and enables counting the number of bytes and the conformance level per packet.

Syntax **traffic-policy** *traffic-policy-def* **count**

no traffic-policy *traffic-policy-def* **count**

Command Default No traffic policy is applied.

Parameters *traffic-policy-def*

Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

Modes Global configuration mode

Usage Guidelines The **no** form of this command deletes a traffic policy definition.

Examples This example configures a traffic policy named TPD and enables counting of bytes and conformance levels.

```
device#configure terminal
device(config)#traffic-policy TPD count
```

traffic-policy rate-limit adaptive

Configures an ACL-based flexible-bandwidth traffic policy to define rate limits on packets so that you can allow for bursts above the limit.

Syntax **traffic-policy** *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **count**

traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action drop** [**count**]

traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **count**

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action drop** [**count**]

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

Command Default No traffic policy is applied.

Parameters *traffic-policy-def*

Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

count

Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

cir *cir-value*

Specifies the committed information rate (CIR) in Kbps, that is, the guaranteed rate of inbound traffic that is allowed on a port. The range is 64 through 1,000,000 Kbps. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The range is 125 through 15,000,000 packets per second.

cbs *cbs-value*

Specifies the committed burst size (CBS), that is, the number of bytes per second allowed on a port before some packets exceed the CIR. You must specify a value greater than 0. On ICX 6650 devices, the *cbs-value* is the rate in packets per second.

pir *pir-value*

Specifies the peak information rate (PIR) in Kbps, that is, the most inbound traffic that is allowed on a port. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The *pir-value*must be equal to or greater than the *cir-value*.

pbs *pbs-value*

Specifies the peak burst size (PBS), that is, the most bytes per second allowed in a burst before all packets exceed the PIR. You must specify a value greater than 0. On ICX 6650 devices, the *pbs-value* is the rate in packets per second.

exceed-action

Specifies the action for traffic that is more than is configured in the *cir-value* variable. If you do not configure this keyword, traffic that exceeds the *cir-value* is dropped

drop

Specifies dropping traffic that exceeds the rate limit.

count

Enables counting the number of bytes and the conformance level per packet. The two-rate three-color marker (trTCM) mechanism described in RFC 2698 is used.

permit-at-low-pri

Specifies permitting packets that exceed the *cir-value* and forward them at the lowest priority.

remark-cos

Sets the 802.1p priority of dropped packets to 0, that is, it sets the COS/PCP field value to 0 for the low priority traffic for any packet exceeding the rate limit set by the traffic policy

Modes Global configuration mode

Usage Guidelines The **no** form of this command deletes a traffic policy definition.

Traffic policies must be referenced by one or more ACLs before they can be effective. The policies are effective on ports to which the ACLs that reference them are bound.

NOTE
You cannot delete a traffic policy definition that a port is currently using. To delete a traffic policy, you must first unbind the associated ACL.

It is recommended that you specify a PBS value that is equal to or greater than the size of the largest possible IP packet in the stream.

Examples This example configures a traffic policy named TPDA4 that specifies a CIR of 10000 Kbps, a CBS of 1600 Kbps, a PIR of 20000 Kbps, and a PBS of 1000 Kbps a and dropping any traffic that exceeds those limits.

```
device#configure terminal
device(config)#traffic-policy TPDA4 rate-limit adaptive cir 10000 cbs 1600 pir
20000 pbs 4000 exceed-action drop
```

traffic-policy rate-limit fixed

Configures an ACL-based fixed-rate traffic policy to define rate limits on packets. It either drops all traffic that exceeds the limit, or forwards it at the lowest priority level.

Syntax **traffic-policy** *traffic-policy-def* **rate-limit fixed** *cir-value* **count**

traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action drop** [**count**]

traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **count**

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action drop** [**count**]

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

Command Default No traffic policy is applied.

Parameters

traffic-policy-def

Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

cir-value

Specifies the committed information rate (CIR) in Kbps, that is, the guaranteed rate of inbound traffic that is allowed on a port. The range is 64 through 1,000,000 Kbps. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The range is 125 through 15,000,000 packets per second

count

Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

exceed-action

Specifies the action for traffic that is more than is configured in the *cir-value* variable. If you do not configure this keyword, traffic that exceeds the *cir-value* is dropped

drop

Specifies dropping traffic that exceeds the rate limit.

count

Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

permit-at-low-pri

Specifies permitting packets that exceed the *cir-value* and forward them at the lowest priority.

remark-cos

Sets the 802.1p priority of dropped packets to 0, that is, it sets the COS/PCP field value to 0 for the low priority traffic for any packet exceeding the rate limit set by the traffic policy

Modes Global configuration mode

Usage Guidelines The **no** form of this command deletes a traffic policy definition.

Traffic policies must be referenced by one or more ACLs before they can be effective. The policies are effective on ports to which the ACLs that reference them are bound.

NOTE
You cannot delete a traffic policy definition that is currently in use on a port. To delete a traffic policy, you must first unbind the associated ACL.

Examples This example configures a traffic policy named TPD1 that specifies a CIR of 100 Kbps and dropping any traffic that exceeds the limit.

```
device#configure terminal
device(config)#traffic-policy TPD1 rate-limit fixed 100 exceed-action drop
```

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 v3 checksum computation method.

Modes VRRP configuration mode

Usage Guidelines The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

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.

Examples The following example shows the v2 checksum computation method enabled in IPv4 and IPv6 VRRPv3 instances.

```
IPv6 :
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv6 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# use-v2-checksum

IPv4 :
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv4 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# version v3
Brocade(config-vif-3-vrid-2)# use-v2-checksum
```

History

Release version	Command history
08.0.01	This command was introduced for IPv6 VRRPv3 sessions running on FastIron device images.
08.0.10b	This command was introduced for IPv4 VRRPv3 sessions running on FastIron device images.

version

Allows you to select either version 2 or version 3 of VRRP.

Syntax **version** {**v2** |**v3**}

no version v3

Command Default The default is VRRP version 2.

Parameters **v2**

Selects version 2 of VRRP.

v3

Selects version 3 of VRRP.

Modes VRRP virtual router ID configuration.

Usage Guidelines You can choose either version 2 or version 3 of IPv4 VRRP. The default IPv4 VRRP configuration is VRRPv2. The VRRPv3 functionality is enabled only after you configure version 3. Use the **no version v3** or **version v2** commands to roll back to the default (VRRPv2).

Examples The following example configures the VRRP owner router for IPv4.

```
device(config)#router vrrp
device(config)#interface ethernet 1/6
device(config-if-1/6)#ip-address 192.53.5.1
device(config-if-1/6)#ip vrrp vrid 1
device(config-if-1/6-vrid-1)#owner
device(config-if-1/6-vrid-1)# version v3 | v2
device(config-if-1/6-vrid-1)#ip-address 192.53.5.1
device(config-if-1/6-vrid-1)#activate
```

The following example configures the VRRP backup router for IPv4.

```
device(config)#router vrrp
device(config)#interface ethernet 1/5
device(config-if-1/5)#ip-address 192.53.5.3
device(config-if-1/5)#ip vrrp vrid 1
device(config-if-1/5-vrid-1)#backup
device(config-if-1/6-vrid-1)# version v3 |v2
device(config-if-1/5-vrid-1)#advertise backup
device(config-if-1/5-vrid-1)#ip-address 192.53.5.1
device(config-if-1/5-vrid-1)#activate
```

History

Release version	Command history
08.0.10	This command was introduced.

vxlan vlan

Configures the VXLAN membership of the port by specifying the VLAN port and VNI for VXLAN mapping.

Syntax **vxlan vlan** *vlan-id* **vni** *vni-id* **l2-tunnel** *tunnel-id*

no vxlan vlan *vlan-id* **vni** *vni-id* **l2-tunnel** *tunnel-id*

Command Default No VXLAN mapping to the tunnel.

Parameters *vlan-id*

Specifies the VLAN ID mapped to the VXLAN segment.

vni *vni-id*

Specifies the VXLAN segment ID to which the VLAN is mapped. This allows the extension of the Layer 2 VLAN segment to a remote location.

l2-tunnel *tunnel-id*

Specifies the Layer 2 tunnel that carries the specified VNI.

Modes Interface configuration mode

Usage Guidelines The command enables VLAN-to-VXLAN translation.

Using the VXLAN maps, a VLAN is mapped to a VNI on a VXLAN Layer 2 tunnel and vice versa. Once the VXLAN mapping is configured, all frames belonging to a given {Port, VLAN} pair are "switched" into the VXLAN Layer 2 tunnel, using the VNI configured in the mapping.

When a VXLAN packet destined to the VXLAN gateway (identified by the UDP destination port) is received, the gateway strips off the VXLAN header. The VNI carried in the VXLAN header identifies the VXLAN segment and assigns a unique outgoing port and a VLAN for the frame.

The **no** form of the command disables VLAN-to-VXLAN translation.

NOTE
No {DMAC, VLAN} based bridging is performed in the E-Line service.

Examples The following example configures the VXLAN mapping to the tunnel:

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# vxlan vlan 10 vni 1010 l2-tunnel 1
```

The details of the VXLAN mapping to the tunnel are displayed in the **show interface ethernet** command output for the specified .

```
device# show interface ethernet 1/1/1
VXLAN mappings:
  vlan 10 vni 1010 L2-Tunnel 1
```

History

Release version	Command history
08.0.10d	This command was introduced.